Kaspersky Security 9.0 for Microsoft Exchange Servers

Administrator's Guide

APPLICATION VERSION: 9.0 MAINTENANCE RELEASE 1
Dear User!

Thank you for choosing our product. We hope that this document will help you in your work and will provide answers regarding this software product.

Warning! This document is the property of Kaspersky Lab ZAO (herein also referred to as Kaspersky Lab): all rights to this document are reserved by the copyright laws of the Russian Federation and by international treaties. Illegal reproduction and distribution of this document or parts hereof result in civil, administrative or criminal liability by applicable law.

Any type of reproduction or distribution of any materials, including translations, is allowed only with the written permission of Kaspersky Lab.

This document, and graphic images related to it, may only be used for informational, non-commercial, and personal purposes.

Kaspersky Lab reserves the right to amend this document without additional notification. You can find the latest version of this document on the Kaspersky Lab website at http://www.kaspersky.com/docs.

Kaspersky Lab assumes no liability for the content, quality, relevance, or accuracy of any third-party materials used herein, or for any potential harm associated with the use of such materials.

Document revision date: 6/08/2015

© 2015 Kaspersky Lab ZAO. All Rights Reserved.

http://www.kaspersky.com
http://support.kaspersky.com
TABLE OF CONTENTS

ABOUT THIS GUIDE ......................................................................................................................... 7
  In this document .......................................................................................................................... 7
  Document conventions ................................................................................................................ 9

SOURCES OF INFORMATION ABOUT THE APPLICATION ................................................................. 10
  Data sources for independent searching ................................................................................. 10
  Discussing Kaspersky Lab applications on the forum ............................................................ 11

KASPERSKY SECURITY 9.0 FOR MICROSOFT EXCHANGE SERVERS ................................................. 12
  Distribution kit ............................................................................................................................ 12
  Hardware and software requirements ....................................................................................... 13

APPLICATION ARCHITECTURE ....................................................................................................... 15
  Application components and their purpose ............................................................................ 15
  Security Server modules .......................................................................................................... 15
  Backup and statistics database ................................................................................................. 16
  DLP database ............................................................................................................................ 17

COMMON APPLICATION DEPLOYMENT SCENARIOS ..................................................................... 18
  Microsoft Exchange Server roles and corresponding protection configurations .............. 18
  Basic application deployment models ..................................................................................... 20
  Deploying the application on a standalone Microsoft Exchange server ............................... 21
  Application deployment in a Microsoft Exchange database availability group .................... 21

INSTALLING AND REMOVING THE APPLICATION ....................................................................... 22
  Application deployment models ............................................................................................... 22
    Scenario of application deployment with the full set of access privileges .......................... 22
    Scenario of application deployment with a limited set of access privileges ....................... 23
  Application setup procedure .................................................................................................... 24
    Step 1. Checking the availability of the required components and installing them .................. 25
    Step 2. Viewing information about the start of the installation and reviewing the End User License Agreement ........................................................................................................ 25
    Step 3. Selecting the installation type ...................................................................................... 25
    Step 4. Selecting application components and modules ....................................................... 25
    Step 5. Setting up the application's connection to the database of Backup and statistics .......... 26
    Step 6. Selecting an account for launching the Kaspersky Security service ......................... 28
    Step 7. Completing installation ............................................................................................... 28
  Application Configuration Wizard ............................................................................................. 28
    Step 1. Adding a key ................................................................................................................ 29
    Step 2. Configuring server protection .................................................................................... 29
    Step 3. Enabling the KSN service .......................................................................................... 29
    Step 4. Configuring the proxy server settings ...................................................................... 30
    Step 5. Configuring notification delivery settings ................................................................. 30
    Step 6. Completing the configuration .................................................................................... 30
  Upgrading from a previous version of the application .............................................................. 30
  Restoring the application ......................................................................................................... 32
  Removing the application ......................................................................................................... 32

APPLICATION INTERFACE ............................................................................................................ 34
  Main window of the Administration Console ........................................................................... 34
  Console tree ............................................................................................................................... 35
  Workspace .................................................................................................................................. 35
  Quick access pane ..................................................................................................................... 35
  Context menu ............................................................................................................................. 36

APPLICATION LICENSING ............................................................................................................... 37
  About the License Agreement .................................................................................................. 37
About the license........................................................................................................................................37
About the key file....................................................................................................................................38
About the license certificate ......................................................................................................................38
About the key ..........................................................................................................................................38
Types of keys used in the application ......................................................................................................38
Licensing options ...................................................................................................................................38
Special considerations of activating the application when using profiles ..............................................39
Special considerations of activating the application when using the key for the DLP Module ...............40
About notifications related to the license ..................................................................................................40
About data submission ..............................................................................................................................40
Activating the application ..........................................................................................................................42
Viewing information about installed keys ..................................................................................................43
Replacing a key ........................................................................................................................................43
Removing a key .......................................................................................................................................44
Configuring the license expiry term notification .......................................................................................45

STARTING AND STOPPING THE APPLICATION .................................................................................46
Starting and stopping a Security Server ....................................................................................................46
Starting the Administration Console ..........................................................................................................46
Adding Security Servers to Administration Console ................................................................................47

SERVER PROTECTION STATUS ........................................................................................................48
Default Microsoft Exchange Server protection .........................................................................................48
Viewing Microsoft Exchange Server protection status details ...............................................................49
Viewing profile protection status details ..................................................................................................53

ROLE-BASED ACCESS ..........................................................................................................................56
MANAGING PROFILES ...........................................................................................................................58
About profiles ............................................................................................................................................58
Creating a profile ....................................................................................................................................59
Configuring Security Servers in a profile ...................................................................................................59
Specifics of managing profiles in a Microsoft Exchange database availability group ................................60
Adding Security Servers to a profile ..........................................................................................................60
Removing a Security Server from a profile ................................................................................................61
Removing a profile ..................................................................................................................................62

UPDATING PROGRAM DATABASES ......................................................................................................63
About program database updates ................................................................................................................63
About update centers ...............................................................................................................................63
About database updates in configurations with a DAG of servers ............................................................64
Updating databases manually ..................................................................................................................64
Configuring scheduled databases updates ..............................................................................................65
Selecting an update source .......................................................................................................................66
Configuring the connection to the update source .....................................................................................67
Configuring proxy server settings ...........................................................................................................67
Designating a server as an update center and configuring its settings .....................................................67

ANTI-VIRUS PROTECTION .....................................................................................................................69
About Anti-Virus protection .....................................................................................................................69
About background scanning .....................................................................................................................70
About participation in Kaspersky Security Network ..................................................................................72
Enabling and disabling anti-virus server protection .................................................................................72
Enabling and disabling KSN in Anti-Virus ...............................................................................................73
Configuring Anti-Virus processing of objects ........................................................................................74
Configuring mailbox and public folder protection settings .....................................................................74
Configuring anti-virus scan exclusions .....................................................................................................75
   About trusted recipients ........................................................................................................................75
   Configuring exclusions by recipient's address .......................................................................................76
   Configuring exclusions by file name mask ..........................................................................................77
Configuring scanning of attached containers and archives .......................................................... 78
Configuring background scan settings ....................................................................................... 78
PROTECTION AGAINST SPAM AND PHISHING ................................................................. 80
About Anti-Spam protection ........................................................................................................ 80
About additional services, features, and anti-spam technologies .............................................. 82
Improving the accuracy of spam detection on Microsoft Exchange 2013 servers ................... 83
About anti-phishing scans ............................................................................................................. 83
Enabling and disabling Anti-Spam protection of the server ....................................................... 83
Enabling and disabling message scanning for phishing ............................................................ 84
Configuring spam and phishing scan settings ............................................................................ 84
Configuring the white and black lists of senders ....................................................................... 86
Configuring the white list of recipients ....................................................................................... 87
Configuring an increase in the spam rating of messages ............................................................ 88
Using external anti-spam message scanning services ................................................................. 90
Configuring additional settings of spam and phishing scans .................................................... 91
BACKUP ................................................................................................................................. 93
About Backup ............................................................................................................................. 93
Viewing the Backup contents ..................................................................................................... 94
Viewing properties of objects in Backup ................................................................................... 94
Filtering the list of Backup objects ............................................................................................. 95
Saving objects from Backup to disk ........................................................................................... 96
Sending an objects from Backup to recipients .......................................................................... 96
Deleting objects from Backup .................................................................................................... 96
Configuring Backup settings ..................................................................................................... 97
Selecting Backup database for viewing its contents from the profile .......................................... 97
DATA LEAK PREVENTION ............................................................................................... 99
About data leak prevention ......................................................................................................... 99
Managing the DLP Module ......................................................................................................... 99
Enabling and disabling Data Leak Prevention ............................................................................ 100
Assigning the DLP query controller server ................................................................................. 100
Configuring the connection to the DLP database ...................................................................... 101
NOTIFICATIONS ..................................................................................................................... 102
About notifications ..................................................................................................................... 102
Configuring notification settings ............................................................................................... 102
Configuring notification delivery settings ................................................................................ 103
REPORTS ............................................................................................................................... 104
About application reports .......................................................................................................... 104
Creating Quick reports ............................................................................................................. 104
Creating a report generation task ............................................................................................... 105
Viewing the list of report generation tasks .................................................................................. 106
Editing the settings of a report generation task .......................................................................... 107
Starting a report generation task ............................................................................................... 107
Deleting a report generation task .............................................................................................. 107
View the Ready reports .............................................................................................................. 108
Saving a report ......................................................................................................................... 109
Deleting a report ....................................................................................................................... 110
APPLICATION LOGS ............................................................................................................. 111
About application logs ............................................................................................................... 111
Configuring log settings ........................................................................................................... 111
Configuring the detail level of logs ........................................................................................... 112
MANAGING CONFIGURATION ......................................................................................... 114
Exporting settings ..................................................................................................................... 114
Importing settings ..................................................................................................................... 115
TESTING THE APPLICATION OPERATION............................................................... 116
  About the EICAR test file.................................................................................. 116
  About the types of the EICAR test file .......................................................... 116
  Testing application performance using the EICAR test file ........................... 117

CONTACTING THE TECHNICAL SUPPORT SERVICE ....................................... 119
  About technical support .................................................................................... 119
  Technical support by phone............................................................................. 119
  Technical Support via Kaspersky CompanyAccount ........................................ 119
  Using a trace file and AVZ script ................................................................... 120

APPENDIX. SCRIPT FOR SENDING SPAM FOR ANALYSIS .............................. 121
  About the script for sending spam for analysis .............................................. 121
  Script operation modes..................................................................................... 121
  Script execution parameters .......................................................................... 122
  Configuring parameters of the script configuration file .................................. 123
  Script operation log ......................................................................................... 124

GLOSSARY ........................................................................................................... 125

KASPERSKY LAB ZAO ......................................................................................... 129

INFORMATION ABOUT THIRD-PARTY CODE ............................................... 130

TRADEMARK NOTICE ....................................................................................... 131

INDEX ............................................................................................................... 132
ABOUT THIS GUIDE

This document is the Administrator’s Guide to Kaspersky Security 9.0 for Microsoft® Exchange Servers (hereinafter also referred to as “Kaspersky Security”).

This Guide is intended for technical specialists tasked with installing and administering Kaspersky Security and supporting companies that use Kaspersky Security.

The Guide serves the following purposes:

- Helps to configure and use the application.
- Serves as a quick source of information to answer questions relating to the operation of Kaspersky Security.
- References additional sources of information about the application and describes ways to get technical support.

In this document

In this document ................................................................. 7
Document conventions ................................................................ 9

IN THIS DOCUMENT

This document includes the following sections:

Sources of information about the application (see page 10)
This section describes sources of information about the application and lists websites that you can use to discuss the application’s operation.

Kaspersky Security 9.0 for Microsoft Exchange Servers (see page 12)
This section describes the features of the application and provides brief information about application functions and components. You will learn what items are included in the distribution kit and what services are available for registered users of the application. This section provides information about the software and hardware requirements that a computer must meet to allow installation.

Application architecture (see page 15)
This section describes Kaspersky Security components and the logic of their interaction.

Basic application deployment models (see page 18)
This section covers the standard models of application deployment on a corporate network and the particulars of integration with third-party software.

Installing and removing the application (see page 22)
This section contains step-by-step instructions for removing and updating the application.

Application interface (see page 34)
This section provides information about the basic elements of the graphical user interface of the application, such as the main window of Administration Console, the tree of Administration Console, the workspace, the quick access pane, and the context menu.

Application licensing (see page 37)
This section contains information about the basic concepts of application activation. This section describes the purpose of the End User License Agreement, the ways to activate the application and renew the license.
Starting and stopping the application (see page 46)
This section contains information on starting and shutting down the application.

Server protection status (see page 48)
This section covers the default settings of Kaspersky Security. This section describes how you can use the Administration Console to view license info, the status of application modules and databases, as well as statistics on the number of messages processed and instances of threats and spam detected.

Role-based access (see page 56)
This section explains how to restrict access to the application using roles.

Managing profiles (see page 58)
This section describes how you can create, manage, and configure profiles.

Updating databases (see page 63)
This section explains how to update application databases and configure database updates.

Anti-virus protection (see page 69)
This section contains information about Anti-Virus protection of a Microsoft Exchange server, background scanning of storages, and ways to configure protect and scan settings.

Anti-Spam and Anti-Phishing protection (see page 80)
This section contains information about Anti-Spam and Anti-Phishing filtering of email traffic and instructions on configuring it.

Backup (see page 93)
This section contains information about Backup and how to use it.

Data Leak Prevention (see page 99)
This section provides information and instructions on how to implement prevention of confidential data leaks via corporate email.

Notifications (see page 102)
This section covers notifications and ways to configure them.

Reports (see page 104)
This section covers application reports and ways to configure them.

Application logs (see page 111)
This section covers the application logs and ways to configure them.

Configuration management (see page 114)
This section explains how you can export the application configuration to file and import it from file.

Application testing (see page 116)
This section explains how to test the application in order to make sure that it detects viruses and their modifications and takes action on them.

Contacting Technical Support (see page 119)
This section explains how to contact Kaspersky Lab Technical Support.

Appendix. Script for sending spam for analysis (see page 121)
This section describes a script for sending spam for analysis to Kaspersky Lab specialists and how to configure it.
Glossary (see page 125)
This section contains a list of terms mentioned in the document and their respective definitions.

Kaspersky Lab ZAO (see page 129)
This section provides information about Kaspersky Lab ZAO.

Information about third-party code (see page 130)
This section provides information about third-party code used in the application.

Trademark notices (see page 131)
This section lists third-party trademarks used in this document.

Index
This section allows you to quickly find required information within the document.

DOCUMENT CONVENTIONS
This document uses the following conventions (see table below).

<table>
<thead>
<tr>
<th>SAMPLE TEXT</th>
<th>DOCUMENT CONVENTIONS DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note that...</td>
<td>Warnings are highlighted in red and enclosed in frames. Warnings show information about actions that may have unwanted consequences.</td>
</tr>
<tr>
<td>It is recommended that you use...</td>
<td>Notes are enclosed in frames. Notes provide additional and reference information.</td>
</tr>
<tr>
<td>Example: ...</td>
<td>Examples are given on a yellow background under the heading &quot;Example&quot;.</td>
</tr>
<tr>
<td>An update is... The Databases are outdated event occurs.</td>
<td>The following elements are italicized in the text: • new terms; • status variations and application events.</td>
</tr>
<tr>
<td>Press ENTER. Press ALT-F4.</td>
<td>Names of keyboard keys appear in bold and are capitalized. Names of keys linked with a + (plus) sign indicate key combinations. These keys have to be pressed simultaneously.</td>
</tr>
<tr>
<td>Click the Enable button.</td>
<td>UI elements, for example, names of entry fields, menu items, buttons are in bold.</td>
</tr>
<tr>
<td>To configure a task schedule, perform the following steps:</td>
<td>Introductory phrases of instructions are printed in italics and marked with an arrow sign.</td>
</tr>
<tr>
<td>Enter help in the command line. The following message will appear: Specify the date in DD:MM:YY format.</td>
<td>The following types of text content are set off with a special font: • command line text; • text of program messages output on the screen; • Data to be entered using the keyboard.</td>
</tr>
<tr>
<td>&lt;User name&gt;</td>
<td>Variables are enclosed in angle brackets. Instead of a variable, the corresponding value should be inserted, with angle brackets omitted.</td>
</tr>
</tbody>
</table>
SOURCES OF INFORMATION ABOUT THE APPLICATION

This section lists the sources of information about the application.
You can select the most convenient source, depending on the urgency or importance of your question.

IN THIS SECTION:

Data sources for independent searching................................................................. 10
Discussing Kaspersky Lab applications on the forum............................................... 11

DATA SOURCES FOR INDEPENDENT SEARCHING

You can use the following sources to find information about the application:

- Application page on the Kaspersky Lab website
- Application page on the Technical Support website (Knowledge Base)
- Online help
- Documentation

If you cannot find the solution to an issue on your own, we recommend that you contact Technical Support at Kaspersky Lab.

To use information sources on the Kaspersky Lab website, an Internet connection should be established.

Application page on the Kaspersky Lab website
The Kaspersky Lab website features an individual page for each application.
Visit: http://www.kaspersky.com/security-microsoft-exchange-servers to view general information about the application, its features and functions.
A link to eStore is available on the http://www.kaspersky.com website. There you can purchase the application or renew your license.

The application page on the Technical Support web site (in the Knowledge Base)
Knowledge Base is a section on the Technical Support website that provides advice on using Kaspersky Lab applications. Knowledge Base comprises reference articles that are grouped by topic.
On the page of the application in the Knowledge Base (http://support.kaspersky.com/kse9), you can read articles that provide useful information, recommendations, and answers to frequently asked questions on how to purchase, install, and use the application.
Articles may provide answers to questions relating not just to Kaspersky Security, but also to other Kaspersky Lab applications. They also may contain news from Technical Support.

Online help
The online help of the application comprises help files.
Online help contains information about each window of the application: the list of settings, their descriptions and links to the tasks using these settings.
Full help provides information about managing computer protection, configuring the application and solving typical user tasks.
Documentation
On this page of the Kaspersky Lab website (http://www.kaspersky.com/product-updates/microsoft-exchange-server-antivirus), you can download documents that will help you to install the application on computers on the corporate network, configure application settings, and find information about the basic techniques for using the application.

**DISCUSSING KASPERSKY LAB APPLICATIONS ON THE FORUM**
If your question does not require an immediate answer, you can discuss it with the Kaspersky Lab experts and other users in our forum (http://forum.kaspersky.com/index.php?showforum=5).
In this forum you can view existing topics, leave your comments, create new topics.
Kaspersky Security 9.0 for Microsoft Exchange Servers is an application designed for protection of mail servers based on Microsoft Exchange Server against viruses, Trojan software and other types of threats that may be transmitted via e-mail, as well as spam, phishing, and accidental leaks of confidential corporate data via email.

Kaspersky Security provides anti-spam protection on the level of your corporate mail server, saving your employees the trouble of deleting unwanted mail manually.

Kaspersky Security protects mailboxes, public folders, and relayed mail traffic on a Microsoft Exchange Server against malware, spam, and phishing. Kaspersky Security scans all e-mail traffic passing through the protected Microsoft Exchange Server.

Kaspersky Security can perform the following operations:

- Scan mail traffic, incoming and outgoing mail, as well as the messages stored on a Microsoft Exchange Server (including public folders) for malware. The scan processes the message and all of its attachments. Depending upon the selected settings, the application disinfects and removes detected harmful objects and provides users with complete information about them.
- Filter unsolicited mail (spam) from mail traffic. The Anti-Spam component scans mail traffic for spam content. In addition, Anti-Spam allows you to create black and white lists of senders' addresses and supports a flexible configuration of anti-spam scanning sensitivity.
- Scan mail traffic for phishing and malicious URLs.
- Prevent leaks of confidential information and information with specific parameters in incoming and outgoing email messages.
- Save backup copies of objects (an object consists of message content and its attachments) and spam messages prior to their disinfection or deletion to enable subsequent restoration, if required, thus preventing the risk of data losses. Configurable filters allow the user to easily locate specific stored objects.
- Notify the sender, the recipient and the system administrator about messages that contain malicious objects.
- Manage identical settings of multiple Security Servers in centralized mode by means of profiles.
- Maintain event logs, display statistics, and create regular reports on application activity. The application can create reports automatically according to a schedule or manually.
- Configure the application settings to match the volume and type of relayed mail traffic, in particular, define the maximum connection wait time to optimize scanning.
- Update the Kaspersky Security databases automatically or in manual mode. Updates can be downloaded from the FTP and HTTP servers of Kaspersky Lab, from a local / network folder that contains the latest set of updates, or from user-defined FTP and HTTP servers.
- Re-scan old (previously scanned) messages for the presence of new viruses or other threats according to a schedule. This task is performed as a background scan and has little effect on the mail server's performance.
- Perform anti-virus protection on storage level based on the list of protected storages.

In this section:

Distribution kit................................................................. 12
Hardware and software requirements ........................................ 13

Distribution Kit

Kaspersky Security is available from online stores of Kaspersky Lab (for example, http://www.kaspersky.com, in the eStore section) and from partner companies.

Kaspersky Security is supplied as part of Kaspersky Security for Mail Servers and Kaspersky Total Security.
After buying a license for Kaspersky Security, you will receive an email with a link for downloading the application from the eStore website along with an application key file, or a CD with the distribution kit containing the application files and manuals.

Before breaking the seal on the envelope with the installation disk, carefully read through the EULA.

For more information about ways to purchase the application and about the distribution kit, contact the Sales Department at sales@kaspersky.com.

**HARDWARE AND SOFTWARE REQUIREMENTS**

For Kaspersky Security to work properly, the computer should meet the hardware and software requirements listed below.

**Hardware requirements**

The hardware requirements for installing the Security Server are identical to the hardware requirements for a protected Microsoft Exchange server, except for the RAM volume.

Hardware requirements for installing the Security Server:

- Processor – according to the hardware requirements for the protected Microsoft Exchange server;
- 4 GB free RAM, including:
  - 2 GB – for the operation of Anti-Virus and Anti-Spam;
  - 2 GB – for the operation of the DLP Module.
- 10 GB of free disk space, including at least 4 GB for the DLP Module's operation. Additional disk space may be required depending on the application settings and operation mode.

The Administration Console is installed together with the Security Server.

The Administration Console can be also installed separately from the Security Server. Hardware requirements for separate installation of the Administration Console:

- Intel® Pentium® 400 MHz or faster processor (1000 MHz recommended);
- 256 MB free RAM;
- 500 MB disk space for the application files.

**Software requirements**

The Security Server can be installed under one of the following operating systems:

- Microsoft Windows Server® 2012 R2 Standard or Datacenter;
- Microsoft Windows Server 2012 Standard or Datacenter;
- Microsoft Windows® Small Business Server 2011 Standard;
- Microsoft Windows Server 2008 SP2 Standard or Enterprise;
- Microsoft Windows Server 2008 R2 SP1 Standard, Enterprise or Datacenter.

The following software is required to install the Security Server:

- One of the following mail servers:
  - Microsoft Exchange Server 2010 SP3 deployed in at least one of the following roles: Hub Transport, Mailbox, or Edge Transport;
  - Microsoft Exchange Server 2013 SP1 deployed in at least one of the following roles: Mailbox, Hub Transport, or Client Access Server (CAS).
- Microsoft .NET Framework 3.5 SP1.
- One of the following database management systems:
  - Microsoft SQL Server 2014® Express, Standard, or Enterprise;
• Microsoft SQL Server 2012 Express, Standard or Enterprise;
• Microsoft SQL Server 2008 R2 Express, Standard or Enterprise;
• Microsoft SQL Server 2008 Express, Standard or Enterprise;

Administration Console can be installed under one of the following operating systems:

• Microsoft Windows 8.1;
• Microsoft Windows Server 2012 R2 Standard or Datacenter;
• Microsoft Windows Server 2012 Standard or Datacenter;
• Microsoft Windows 8;
• Microsoft Windows Small Business Server 2011 Standard;
• Microsoft Windows 7 SP1 Professional, Enterprise or Ultimate;
• Microsoft Windows Server 2008 SP2 Standard or Enterprise;
• Microsoft Windows Server 2008 R2 SP1 Standard, Enterprise or Datacenter;
• Microsoft Windows Vista® Business, Enterprise or Ultimate.

Installation of the Administration Console requires the following software:

• Microsoft Management Console 3.0;
• Microsoft .NET Framework 3.5 SP1.
APPLICATION ARCHITECTURE

This section describes Kaspersky Security components and the logic of their interaction.

IN THIS SECTION:

Application components and their purpose ................................................................. 15
Security Server modules ............................................................................................. 15
Backup and statistics database ..................................................................................... 16
DLP database .................................................................................................................. 17

APPLICATION COMPONENTS AND THEIR PURPOSE

Kaspersky Security consists of two basic components:

- **Security Server** is installed on a Microsoft Exchange server and focuses on filtering mail traffic to clear it of spam and phishing, protect it against viruses, and prevent data leaks in outgoing and internal messages. Security Server intercepts messages coming to the Microsoft Exchange Server and scans them for viruses, spam, and data leaks with Anti-Virus, Anti-Spam, and DLP Module, respectively. If a message coming to the Microsoft Exchange server turns out to be infected with a virus, contain spam, or shows a data leak, the application performs the actions specified in the settings of the relevant module.

- The **Administration Console** is a dedicated isolated snap-in integrated into Microsoft Management Console 3.0. You can use the Administration Console to create and edit the list of protected Microsoft Exchange servers and manage Security Servers. The Administration Console can be installed either on a Microsoft Exchange server together with the Security Server or on a remote computer (see section "Deploying the application on a standalone Microsoft Exchange server" on page 21).

SECURITY SERVER MODULES

Security Server consists of the following modules:

- **E-mail Interceptor.** Intercepts messages arriving on the Microsoft Exchange server and forwards them to Anti-Virus and Anti-Spam. This module is integrated into Microsoft Exchange processes using either VSAPI 2.6 or Transport Agents technology depending on the role in which the Microsoft Exchange server has been deployed.

  When installing Kaspersky Security, a transport agent named Kaspersky Antispam filter agent is registered on the Microsoft Exchange server that has the highest priority. Do not change the priority of this transport agent. Doing so may reduce the effectiveness of protection.

- **Anti-Virus.** Scans messages for viruses and other malicious objects. This module comprises an anti-virus kernel and a storage for temporary objects, which is used for scanning objects in RAM. The storage is located in the working folder Store.

  The Store folder is created in the application data storage folder (by default: <application setup folder>/data). You have to exclude it from scanning by anti-virus applications installed on the corporate network. Otherwise, Kaspersky Security may operate incorrectly.

- **Anti-Spam.** Filters out unsolicited mail. After intercepting a message, E-mail Interceptor relays it for processing by Anti-Spam. Copies of deleted messages can be stored in Backup.

- **DLP Module.** Monitors leaks of confidential data and data with special characteristics in outgoing email messages.

- **Internal Application Management and Integrity Control Module.** It is the Kaspersky Security 9.0 for Microsoft Exchange Servers service in Microsoft Windows. The module is started automatically when the first message passes through the Microsoft Exchange server;
This service does not depend on the state of the Microsoft Exchange Server (whether it is started or stopped), so the application can be configured when the Microsoft Exchange Server is stopped.

The Internal Application Management and Integrity Control Module should be running at all times. Do not end the Kaspersky Security 9.0 for Microsoft Exchange Servers service manually, as this will disable the Security Server and stop the scanning process.

**Backup and Statistics Database**

The application stores Backup data and application statistics in a special database deployed on a Microsoft SQL Server, the so-called **Backup and statistics database** (hereinafter also database).

On being installed, the application can create a new database or use an existing database. When the application is removed, the database can be saved on an SQL server for future use.

The Backup and statistics database can be stored locally on one computer with the Security Server or on a remote computer on the corporate LAN.

Kaspersky Security does not encrypt data transmitted between the Security Server and the database. When the database is hosted on a remote computer, you have to manually encrypt data transmitted via communication channels if such encryption is required by the information security policy of your company.

Some part of the application configuration data are stored in the database. The application does not control unauthorized modification of those data nor their integrity. You will have to take your own steps in order to protect the data against unauthorized access and control the data integrity.

**Database settings**

The Backup and statistics database settings are stored in the following configuration file:

```
<application setup folder>/Configuration/BackendDatabaseConfiguration.config
```

It is an editable XML file. It contains the following settings:

- **SqlServerName** : name of the SQL server. It is specified by the application automatically as `<SQL server name>` based on information provided by the administration during installation of the application.

- **DatabaseName** – name of the main database. It is specified by the application automatically based on information provided by the administration during installation of the application.

- **FailoverPartner**: settings (SQL server and instance) of the database mirror. They are specified by the application automatically as `<SQL server name>`.

We strongly advise against changing the names of the SQL server and primary database during operation of the application. The application should be stopped before such modifications are made. Otherwise, the Backup and statistics database data will be partly lost.

Changes made to the configuration file become effective within one minute.

**Database mirroring**

The application supports the Database Mirroring technology. If this technology is used in the configuration of your SQL server, the application will use it automatically. In other words, if the main Backup and statistics database fails or is disabled, the application automatically switched to using a database mirror. The application automatically switches back to the primary database as soon as it has been restored.
DLP DATABASE

The application stores data of DLP Module (see page 99), such as data of policies, incidents, user categories, as well as statistics of DLP Module, in the DLP database.

The DLP database is operated with Microsoft SQL Server. By default, the DLP database is deployed along with the database of Backup and statistics. You can export tables from the DLP database to another database under a different name or deploy DLP databases on a different SQL server (see the section “Configuring connection to the DLP database” on page 101).

Depending on the intensity of the mail flow in your organization and the settings of policies that determine the number of incidents to be created, the DLP database may have a significant volume. This should be taken into account when planning the deployment of the DLP database. To reduce the size of the DLP database, you can use the incident archiving feature (please refer to the Security Officer’s Guide to Kaspersky Security 9.0 for Microsoft Exchange Servers for detailed information).
COMMON APPLICATION DEPLOYMENT SCENARIOS

This section describes the Microsoft Exchange mail infrastructure configurations in which Kaspersky Security can be deployed.

In this section:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Exchange Server roles and corresponding protection configurations</td>
<td>18</td>
</tr>
<tr>
<td>Basic application deployment models</td>
<td>20</td>
</tr>
<tr>
<td>Deploying the application on a standalone Microsoft Exchange server</td>
<td>21</td>
</tr>
<tr>
<td>Application deployment in a Microsoft Exchange database availability group</td>
<td>21</td>
</tr>
</tbody>
</table>

MICROSOFT EXCHANGE SERVER ROLES AND CORRESPONDING PROTECTION CONFIGURATIONS

The set of application modules that can be installed depends on the role in which the Microsoft Exchange Server has been deployed.

Successful installation of Kaspersky Security on a Microsoft Exchange 2010 server requires the Microsoft Exchange server to be deployed in at least one of the following roles:

- Mailbox (Mailbox Server).
- Hub Transport Server.
- Edge Transport. Server
The following figure shows a chart for interaction between the components of Kaspersky Security and a Microsoft Exchange server when installing Kaspersky Security on a Microsoft Exchange 2010 server.

Successful installation of Kaspersky Security on a Microsoft Exchange 2013 server requires the Microsoft Exchange server to be deployed in at least one of the following roles:

- Mailbox (Mailbox Server).
- Client Access® Server (CAS).
- Edge Transport. Server
The following figure shows a chart for interaction between the components of Kaspersky Security and a Microsoft Exchange server when installing Kaspersky Security on a Microsoft Exchange 2013 server.

**Figure 2: Flowchart of interaction between Kaspersky Security components and the Microsoft Exchange 2013 server**

If Microsoft Exchange Server 2010 is deployed in the Mailbox role, Kaspersky Security interacts with it using the VSAPI 2.6 standard. In other cases, the Transport Agents technology is used for integration with the Microsoft Exchange Server. Please note that in the Hub Transport role, messages are first scanned by the application and then processed by Microsoft Exchange Transport Agents. In the Edge Transport role, the procedure is reversed – messages are first processed by Microsoft Exchange Transport Agents and then by the application.

**BASIC APPLICATION DEPLOYMENT MODELS**

You can choose one of the two application deployment models depending on your corporate Microsoft Exchange infrastructure:

- The Security Server is installed on the computer hosting the Microsoft Exchange server. The Administration Console can be installed on the same computer or on any other computer on the corporate network for remote management of the Security Server (see section "Deploying the application on a standalone Microsoft Exchange server" on page 21).
- The Security Server is installed in the Database Availability Group (hereinafter also "DAG") (see section "Application deployment in a Microsoft Exchange database availability group" on page 21). In this case, the Security Server and Administration Console should be installed together on each Microsoft Exchange server belonging to the DAG.
DEPLOYING THE APPLICATION ON A STANDALONE MICROSOFT EXCHANGE SERVER

The application can be installed on one or several standalone Microsoft Exchange servers. Security Server and Administration Console used to manage Security Server can be installed on the same Microsoft Exchange server.

If necessary, you can install the Administration Console separately from the Security Server on any computer on the corporate network for remote management of the Security Server. If several administrators are working jointly, the Administration Console can be installed on each administrator's computer.

Administration Console connects to the Security Server via TCP port 13100. You have to open this port in the firewall on the remote Microsoft Exchange server or add the service of Kaspersky Security 9.0 for Microsoft Exchange Servers to the list of trusted applications of the firewall.

APPLICATION DEPLOYMENT IN A MICROSOFT EXCHANGE DATABASE AVAILABILITY GROUP

Kaspersky Security can be installed on servers belonging to a Microsoft Exchange Database Availability Group (DAG).

During installation, the application automatically recognizes the database availability group. The order in which the application is installed on nodes within the DAG is irrelevant.

The specifics of Kaspersky Security installation in the DAG are as follows:

- You should use a single database for all DAG nodes. This requires specifying a single database during Kaspersky Security installation on all nodes of the DAG.
- The account used to perform the installation procedure must be authorized to write to the Active Directory configuration section.
- If a firewall is enabled on the DAG servers, the Kaspersky Security 9.0 for Microsoft Exchange Servers service must be added to the list of trusted applications on each server within the DAG. This is necessary to ensure the interaction between Kaspersky Security and Backup.

While the previous version of the application is being updated on all servers that are part of the DAG, it is strongly recommended to refrain from connecting to these servers using the Administration Console or editing application settings. Doing so may cause the update to end in an error, which may result in application malfunctions. If the connection needs to be established during an update, before connecting make sure that the Security Server version matches the version of the Administration Console used for establishing the connection.

After installation to a DAG, most of the application settings are stored in the Active Directory, and all DAG servers use those parameters. Kaspersky Security automatically detects active servers and applies the Active Directory settings to them. However, individual settings of the Microsoft Exchange Server have to be configured manually for each DAG server. Examples of individual settings of the Microsoft Exchange Server include: anti-virus protection settings for the Hub Transport role, anti-spam scan settings, Backup settings, settings of the Anti-Spam and Anti-Virus reports for the Hub Transport role, and Anti-Spam database update settings.

Using profiles to configure DAG servers has the following particularities:

- You can add DAG servers to a profile only all at once.
- When a DAG is added to a profile, all servers and all their roles (including the Hub Transport role) are added to this profile.
- You can remove DAG servers from a profile only all at once.

After removing Kaspersky Security from DAG servers, the configuration is stored in Active Directory and can be used to reinstall the application.
INSTALLING AND REMOVING THE APPLICATION

This section provides step-by-step instructions for installing and removing Kaspersky Security.

IN THIS SECTION:
- Application deployment models .......................................................... 22
- Application setup procedure ............................................................... 24
- Application Configuration Wizard ......................................................... 28
- Upgrading from a previous version of the application .............................. 30
- Restoring the application .................................................................. 32
- Removing the application .................................................................. 32

APPLICATION DEPLOYMENT MODELS

Before deploying the application, prepare the following accounts:

- Account for installing the application. The Application Setup Wizard and the Application Configuration Wizard are started under this account.
- Account for launching the application service. If the SQL server is hosted by the same computer on which the application is installed, the role of this account can be performed by the Local System account. In this case, you do not need to create a special account for launching the service.
- Account for preparing the database. Under this account, the Installation Wizard prepares the application database on the SQL server. This account is not used after the installation has been completed.

In order for the application to work properly, TCP port 13100 must be opened on all computers that will host the Security Server and Administration Console as well as along the path of data transmission between them.

You can deploy the application under one of the following scenarios:

- Scenario of application deployment with the full set of access privileges.
- Scenario of application deployment with a limited set of access privileges.

SCENARIO OF APPLICATION DEPLOYMENT WITH THE FULL SET OF ACCESS PRIVILEGES

This deployment scenario is suitable for you if you have sufficient privileges to perform all installation operations on your own without the assistance of other specialists and if your account has the appropriate set of access rights.

To deploy the application with the full set of access rights:

1. Make sure that the account intended for deploying the application is included in the local "Administrators" group on the Microsoft Exchange server on which you are deploying the application. If not, include the account in this group.

2. Make sure that the account intended for deploying the application is included in the "Domain Administrators" and "Enterprise Administrators" groups. If not, include the account in these groups. This is needed in order for the Installation Wizard to be able to create a configuration storage and a role-based access group in Active Directory.
3. Assign the sysadmin role on the SQL server to the account intended for preparing the database. These rights are required to create and configure the database.

4. Add the account intended for launching the service to the local "Administrators" group on the Microsoft Exchange server on which you are deploying the application.

5. Add the account intended for launching the service to the Organization Management group. This is required for the application to retrieve the configuration settings of the Microsoft Exchange server.

6. Launch the Installation Wizard (see section "Application setup procedure" on page 24) and Application Installation Wizard (see section "Application Configuration Wizard" on page 28) and perform their steps.

7. Assign roles to accounts that belong to users that perform duties of administrators and security officers (see section "Role-based access" on page 56):
   - Include the administrator accounts in the group of Kse Administrators accounts.
   - Include the accounts of security officers in the group of Kse Security Officers accounts.

8. Perform replication of Active Directory data across the entire organization. This is required in order for application settings saved in Active Directory to become available for subsequent installations of the application on other Microsoft Exchange servers at your organization.

**Scenario of Application Deployment with a Limited Set of Access Privileges**

This deployment scenario is suitable for you if the security policy of your organization does not allow performing all application installation operations under your account and restricts access to the SQL server or Active Directory. For example, this can happen when the database at your organization is administered by a different specialist with full access to the SQL server.

**To deploy the application with a limited set of access rights:**

1. Make sure that the account intended for deploying the application is included in the local "Administrators" group on the Microsoft Exchange server on which you are deploying the application. If not, include the account in this group.

2. Create the following container in Active Directory:

```
CN=KasperskyLab,CN=Services,CN=Configuration,DC=domain,DC=domain
```

3. Configure full access to this container and to all of its sub-containers for the account intended for installing the application.

4. Create a group of Kse Watchdog Service accounts. The type of group is "Universal". Include in this group the account intended for launching the application service. If a Local System account is used as this account, also include in the Kse Watchdog Service group the account of the computer on which installation is performed.

5. Add the Kse Watchdog Service group to the local "Administrators" group on the Microsoft Exchange server on which you are deploying the application.

6. Provide the Kse Watchdog Service group with the rights to read data from the Active Directory container, which stores the configuration data of Microsoft Exchange:

```
CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=domain,DC=domain
```

7. (Available for Microsoft Exchange 2013 servers only). Provide the Kse Watchdog Services group with the ms-Exch-Store-Admin right. To do this, run the following command in the Exchange Management Shell console:

```
Add-ADPermission -Identity "<path to container with configuration of Microsoft Exchange>" -User "<domain name>\\Kse Watchdog Service" -ExtendedRights ms-Exch-Store-Admin
```

**E.g.:**

```
Add-ADPermission -Identity "CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=domain,DC=domain" -User "domain\\Kse Watchdog Service" -ExtendedRights ms-Exch-Store-Admin
```
8. Provide the Kse Watchdog Service group with the right to run under a different name (impersonation). To do
this, run the following command in the Exchange Management Shell console:

```cmd
New-ManagementRoleAssignment -Name KSE_IMPERSONATION -Role applicationImpersonation -SecurityGroup "Kse Watchdog Service"
```

9. Create the Kse Administrators and Kse Security Officers groups of accounts. These groups can be created in
any domain of the organization. The type of groups is "Universal".

10. Perform replication of Active Directory data across the entire organization.

11. Assign roles to accounts that belong to users that perform duties of administrators and security officers (see
section "Role-based access" on page 56):

   - Include the administrator accounts in the group of Kse Administrators accounts. Also include the account
     for installing the application in this group.
   - Include the accounts of security officers in the group of Kse Security Officers accounts.

12. Ensure creation of the application database. Perform this operation on your own or delegate it to an authorized
specialist.

13. Ensure that the Kse Watchdog Service group of accounts is assigned the db_owner role with respect to the
application database.

14. Provide the following: an account intended for preparing the database, the db_owner role to be applied to the
application database, and the "ALTER ANY LOGIN" right to be applied to the SQL server.

15. Ensure that the steps of the Installation Wizard (see section “Application setup procedure” on page 24) and
Application Configuration Wizard (see section “Application Configuration Wizard” on page 28) are performed
under the account intended for installing the application.

16. Perform replication of Active Directory data across the entire organization. This is required in order for
application settings saved in Active Directory to become available for subsequent installations of the application
on other Microsoft Exchange servers at your organization.

**APPLICATION SETUP PROCEDURE**

During Kaspersky Security installation, services of MSExchangeTransport and MSExchangeIS will need to be restarted.
Services will be restarted automatically without additional prompts.

Kaspersky Security is installed using a setup wizard that guides the user through every step of the setup process. The
**Back** and **Next** buttons can be used to navigate between the screens of the Setup Wizard. The **Cancel** button allows
you to exit the setup wizard.

Before starting installation of the application, make sure that you have completed all the required preparations.

➢ **To start installation of the application,**
run the setup.exe file from the application installation package.
This opens the welcome window of the install package.

**In this section:**

- Step 1. Checking the availability of the required components and installing them ........................................... 25
- Step 2. Viewing information about the start of the installation and reviewing the End User License Agreement .......... 25
- Step 3. Selecting the installation type ................................................................................................................. 25
- Step 4. Selecting application components and modules .......................................................................................... 25
- Step 5. Setting up the application’s connection to the database of Backup and statistics ..................................... 26
- Step 6. Selecting an account for launching the Kaspersky Security service .......................................................... 28
- Step 7. Completing installation ............................................................................................................................ 28
**Step 1. Checking the availability of the required components and installing them**

The welcome screen of the installation package checks if the required components are installed. If the components are not installed, you can do one of the following:

- Download and install the .Net Framework 3.5 SP1 component by clicking the Download and install .Net Framework 3.5 SP1 link (if the component is not installed already).

  The computer must be restarted after .NET Framework 3.5 SP1 installation. If you continue setup without restarting, it may cause problems in the operation of Kaspersky Security.

- Download and install the required component Microsoft Management Console 3.0 by clicking the Download and install MMC 3.0 link (if the component is not installed).

  Microsoft Management Console 3.0 (MMC 3.0) is a part of the operating system in Microsoft Windows Server 2003 R2 and later versions. To install the application on earlier versions of Microsoft Windows Server, update the Microsoft Management Console to version 3.0 by clicking the Download and install MMC 3.0 link.

Click the Kaspersky Security 9.0 for Microsoft Exchange Servers link to start the setup wizard. This opens the welcome window of the install wizard.

**Step 2. Viewing information about the start of the installation and reviewing the End User License Agreement**

In the welcome screen of the setup wizard, view information about the start of Kaspersky Security installation on your computer, and click the Next button to proceed to the window with the End User License Agreement. License Agreement is an agreement between the application user and Kaspersky Lab.

Select the I accept the terms of the License Agreement check box, thereby confirming that you have read the License Agreement and accept its terms and conditions.

Kaspersky Security cannot be installed if you do not accept the terms and conditions of the End User License Agreement.

**Step 3. Selecting the installation type**

At this step, select the type of application installation:

- **Typical.** In this case, the setup wizard installs all of the available application components. During installation, the setup wizard uses the default paths to the setup folder and data folders. If you choose this type of installation, the Setup Wizard proceeds to the Creating database window (see section "Step 5. Setting up the application's connection to the database of Backup and statistics" on page 26).

- **Custom.** In this case, at the next step of the Setup Wizard you can select the application components to be installed, and the destination folder for application installation, and data folders. If you choose this type of installation, the Setup Wizard proceeds to the Custom installation window (see section "Step 4. Selecting application components and modules" on page 25).

**Step 4. Selecting application components and modules**

At this step, you have to select the application components and modules to be installed, and specify the paths to the setup folder and data folders. The set of components and modules available for installation varies depending on whether a Microsoft Exchange server is installed on the computer and on the roles in which it has been deployed (see section "Microsoft Exchange Server roles and corresponding protection configurations" on page 18).
Table 2. Components and modules available for installation on the Microsoft Exchange 2010 server

<table>
<thead>
<tr>
<th>ROLE OF THE EXCHANGE 2010 SERVER</th>
<th>ADMINISTRATION CONSOLE</th>
<th>ANTI-SPAM</th>
<th>ANTI-VIRUS FOR THE MAILBOX ROLE</th>
<th>ANTI-VIRUS FOR THE HUB TRANSPORT ROLE</th>
<th>DLP MODULE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailbox Server.</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hub Transport. Server</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Edge Transport Server.</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

Table 3. Components and modules available for installation on the Microsoft Exchange 2013 server

<table>
<thead>
<tr>
<th>ROLE OF THE EXCHANGE 2013 SERVER</th>
<th>ADMINISTRATION CONSOLE</th>
<th>ANTI-SPAM</th>
<th>ANTI-VIRUS FOR THE MAILBOX ROLE</th>
<th>CAS INTERCEPTOR</th>
<th>ANTI-VIRUS FOR THE HUB TRANSPORT ROLE</th>
<th>DLP MODULE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Access Server (CAS).</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mailbox Server.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Edge Transport Server.</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

The CAS Interceptor module can be selected only if the Microsoft Exchange 2013 server is deployed in the Client Access Server (CAS) role alone.

The CAS Interceptor module is designed to improve spam detection. It is recommended for installation on all Microsoft Exchange 2013 servers deployed in the Client Access Server (CAS) role only. This module is installed automatically together with the Anti-Spam module on Microsoft Exchange 2013 servers deployed in the Mailbox role (if you choose to install Anti-Spam).

Select the application components and modules that you want to install. To cancel your selection of components and return to the default selection, click the Reset button.

To view information about the availability of free disk space needed for the installation of the selected components on the local drives, click the Disk usage button.

The path to the default installation folder is displayed in the lower part of the window in the Destination folder field. If necessary, specify a different destination folder. To do so, click Browse and select a folder in the window that opens.

The Data storage folder field below shows the default path to the application data storage folder. This folder is intended for temporary storage of objects to be scanned and auxiliary files. If necessary, specify a different data folder. To do so, click Browse and select a folder in the window that opens.

When DLP Module is running, the data storage folder may have a significant size. If DLP Module has been selected for installation, you are recommended to allocate the data storage folder on an individual disk.

**STEP 5. SETTING UP THE APPLICATION’S CONNECTION TO THE DATABASE OF BACKUP AND STATISTICS**

At this step, you have to configure the settings of the application connection to the SQL database (also referred to as database) used to store configuration settings of the application and Backup data. You can create a new database of Backup and statistics or use an existing one.

If the connection is to a remote SQL server, make sure that the remote SQL server is enabled to support TCP/IP as a client protocol.
Configure the settings of the connection to the database:

- **In the Name of SQL server field** specify the name (or IP address) of the computer where SQL server is installed, and the SQL server instance, for example, MYCOMPUTER\SQLEXPRESS.

To select an SQL server in the network segment where the computer is located, click the **Browse** button opposite the Name of SQL server field.

The relevant SQL server may be missing from the list of SQL servers if the service of the SQL server browser is not running on the computer hosting the SQL server.

- **In the Database name field**, specify the name of the SQL database where the application will store the Backup data, statistical information and its configuration information.

If the SQL server contains no database with the specified name, it will be created automatically by the setup wizard.

If you plan to use a centralized Backup and centralized storage of statistical data for several Security Servers, the same SQL server and database names must be specified for all the Security Servers. In this case, when installing the application on the second and subsequent Security Servers, specify the name of the database created during application installation on the first Security Server. If you do not intend to use centralized storages, you can specify your own SQL database for each Security Server.

If you deploy Kaspersky Security in a DAG of Microsoft Exchange servers, you are strongly recommended to use a single SQL database for all of the Security Servers.

- **Select an account under which you want to create a database or connect to a database on an SQL server:**
  - **Active account.** In this case, the database is created or connection to a database is performed under the active account.
  - **Other account.** In this case, the database is created or connection to a database is performed under a different account. You must specify the account name and password. You can also select an account by clicking the Browse button.

The selected account must have the following access rights:

- To create a new database, the account must be assigned the dbcreator and securityadmin roles on the SQL server.
- For operations with an existing database the selected account must have the following privileges:

<table>
<thead>
<tr>
<th>BASE PROTECTED ENTITY</th>
<th>PERMISSION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>SERVER</td>
<td>ALTER ANY LOGIN.</td>
<td>The right to create, modify, and delete accounts on the SQL server.</td>
</tr>
<tr>
<td>DATABASE</td>
<td>CREATE TABLE</td>
<td>The right to add tables in the selected database.</td>
</tr>
<tr>
<td>DATABASE</td>
<td>CREATE XML SCHEMA COLLECTION</td>
<td>The right to create collections of XML schemas in the selected database.</td>
</tr>
<tr>
<td>DATABASE</td>
<td>CREATE TYPE</td>
<td>The right to create types in the selected database.</td>
</tr>
<tr>
<td>SCHEMA</td>
<td>CONTROL</td>
<td>The right to control the dbo schema in the selected database.</td>
</tr>
</tbody>
</table>

*Table 4. The privileges for connection to an existing database*

If a new database is created, the application automatically sets these permissions for the selected account.
**STEP 6. SELECTING AN ACCOUNT FOR LAUNCHING THE KASPERSKY SECURITY SERVICE**

At this step, specify the account to be used for launching the application service and connecting Kaspersky Security to the SQL server:

- **Local System account.** In this case the application service will be started and the connection to the SQL server established under the local system account.
- **Other account.** In this case the application service will be started and the connection to the SQL server established under a different account. You must specify the account name and password. You can also select an account by clicking the **Browse** button.

The specified account must possess the required rights.

**STEP 7. COMPLETING INSTALLATION**

At this step, the application files are copied to the computer, the components are registered in the system, and temporary files are removed from Backup.

Click the **Install** button in the Setup Wizard window.

The Setup Wizard starts copying the application files to the computer, registering the components in the system, creating a database on the SQL server (if you chose to create a new database), and restarting the MSExchangeTransport and MSExchangeIS services.

MSExchangeTransport and MSExchangeIS services will be restarted automatically without additional prompts.

Once the files are copied and the components are registered in the system, the Setup Wizard displays a notification about the completed application installation.

To finish the installation, click the **Next** button.

The application configuration wizard starts automatically (see page 28). The application configuration wizard makes it possible to perform initial configuration of application settings.

**APPLICATION CONFIGURATION WIZARD**

The Application Configuration Wizard lets you configure the minimum range of settings needed to build a system for centralized management of server protection.

The Application Configuration Wizard helps to:

- Install a key
- Configure the settings of server protection by the Anti-Virus and Anti-Spam components
- Enable the use of Kaspersky Security Network (hereafter, also KSN)
- Configure the proxy server
- Select the notification method

The Application Configuration Wizard starts automatically when installation is completed. It provides instructions to be followed at every step. The **Back** and **Next** buttons can be used to navigate between the Application Configuration Wizard screens. You can exit the Application Configuration Wizard at any step by closing its window.

You can skip configuring the application and exit the Application Configuration Wizard by clicking the **Cancel** button in the welcome window of the Application Configuration Wizard. You can configure the application in its Administration Console after launching the application.
In this section:

Step 1. Adding a key ................................................................. 29
Step 2. Configuring server protection ........................................ 29
Step 3. Enabling the KSN service .............................................. 29
Step 4. Configuring the proxy server settings .............................. 30
Step 5. Configuring notification delivery settings ......................... 30
Step 6. Completing the configuration ....................................... 30

Step 1. Adding a key

At this step, you can add a key for Kaspersky Security. You can also skip this step and install a key later, after the Application Configuration Wizard finishes and the application launches.

If no key has been added, Kaspersky Security works in "Administration only" mode without protecting the server. To use Kaspersky Security in full functionality mode, you must add a key.

If you deploy Kaspersky Security on a Microsoft Exchange DAG, it suffices to install the key just once during application installation on any of the servers within this DAG. Once this is done, the Application Configuration Wizard will automatically detect the installed key during application installation on other servers within this DAG. In this case, you do not have to add keys for other servers.

Press the Add button. In the displayed File name dialog specify path to the key file (file with the .key extension) and click Open.

They key is installed as the active key. The active key lets you use Kaspersky Security for the duration of the license validity period on the terms of the End User License Agreement.

Step 2. Configuring server protection

At this step, you can configure the settings of server protection against viruses and spam. The Anti-Virus and Anti-Spam modules start working as soon as you launch the application. Anti-Virus and Anti-Spam protection is enabled by default. Enforced Anti-Spam Updates Service and the automatic databases updates are also used by default.

The Enforced Anti-Spam Updates Service requires the computer hosting the Security Server to have a constant Internet connection.

If you do not want Anti-Virus and Anti-Spam to start working as soon as the application is launched, clear the Enable Anti-Virus protection and Enable Anti-Spam protection check boxes. You can enable protection later using the Administration Console.

To disable Enforced Anti-Spam Updates Service, clear the Enable Enforced Anti-Spam Updates Service check box.

To disable automatic updates of Anti-Spam and Anti-Virus databases from Kaspersky Lab servers as soon as the application is launched, clear the Enable automatic database updating check box.

Step 3. Enabling the KSN service

At this step, you can enable the use of the KSN (Kaspersky Security Network) service for spam processing. This window appears only if you have selected the Anti-Spam component for installation (see section "Step 4. Selecting application components and modules" on page 25).

Kaspersky Security Network (KSN) is an infrastructure of online services providing access to Kaspersky Lab's online knowledge base with information about the reputation of files, online resources, and software. The use of data from Kaspersky Security Network ensures faster response by Kaspersky Security to new threats, improves the effectiveness of some protection components, and reduces the risk of false positives.

Access to the KSN service is regulated by a special Kaspersky Security Network Statement. You can review the full text of the Kaspersky Security Network Statement in a separate window by clicking the KSN Statement button.

To use KSN for spam analysis, select the I accept the KSN statement and I want to use KSN check box, thereby confirming that you have read the Kaspersky Security Network Statement and accept its terms.
**STEP 4. CONFIGURING THE PROXY SERVER SETTINGS**

At this step, you can configure proxy server settings. The application uses these settings to connect to Kaspersky Lab update servers while updating application databases and to connect to Kaspersky Security Network.

If you want the application to connect to Kaspersky Lab servers via a proxy server, select the **Use proxy server** check box and specify the settings of the connection to the proxy server in the relevant fields: proxy server address and port. The default port number is 8080.

To use authentication on the proxy server you have specified, select the **Use authentication** check box and enter the relevant information about the user account selected for that purpose in the **Account** and **Password** fields. Use the **button to select one of the existing accounts.

**STEP 5. CONFIGURING NOTIFICATION DELIVERY SETTINGS**

At this step, you can configure notification delivery settings. Notifications enable you and other persons whom they concern to learn about all Kaspersky Security events in a timely fashion. Notifications are sent by email. The following settings have to be specified for successful delivery of notifications: address of the web service and account settings.

In the **Exchange web service address** field specify the address of the web service used for sending emails via the Microsoft Exchange Server (by default, Microsoft Exchange Server uses the following address: https://<name_of_client_access_server>/ews/exchange.asmx).

Specify any account registered on the Microsoft Exchange Server in the **Account** field manually by clicking the **Browse** button, and enter the password of the selected account in the **Password** field.

Enter in the **Administrator address** field the destination mail address, for example, your e-mail.

Click the **Test** button to send a test message. If the test message arrives in the specified mailbox, it means that delivery of notifications is configured properly.

**STEP 6. COMPLETING THE CONFIGURATION**

At this step, the configured application settings are saved and the configuration process finishes.

By default, the Administration Console launches automatically after the configuration has been completed. To disable the automatic launch of the Administration Console, clear the **Start Administration Console after Application Configuration Wizard completion** check box.

Click the **Finish** button to exit the Application Configuration Wizard.

**UPGRADING FROM A PREVIOUS VERSION OF THE APPLICATION**

Kaspersky Security supports the update of the previous version 9.0 to the current version of the application. Upgrading from earlier versions is not supported.

- It is recommended to update the application in a sequence on all Security Servers and Administration Console deployed on the corporate network. If the application update has failed on any Security Server, you will be able to connect to this Security Server only using the Administration Console of the previous version.
- It is recommended to update the application on Microsoft Exchange servers running within a DAG configuration as soon as possible.
- If your organization uses the DLP Module, you are advised to begin upgrading the application with the Security Server that is the DLP query controller server (see section "Assigning the DLP query controller server" on page 100).

SQL server hosting the application database must remain accessible during the update procedure. Otherwise the update will fail.
In order for the application to work properly, TCP port 13100 must be opened on all computers where the application will be upgraded as well as along the path of data transmission between them.

During upgrade of Kaspersky Security, restart of MSExchangeTransport service and MSExchangeIS service is required. Services will be restarted automatically without additional prompts.

Parameter values and data of the previous application version will be transferred to the new version as follows:

- The license for the previous version of the application remains effective for the new version. The end date of the license validity period remains unchanged.
- Application settings configured in the previous version will be applied without changes to the corresponding settings in the new version.
- The value of the maximum size of objects scanned by the Anti-Spam component is set as follows:
  - The value of this setting remains without change if the administrator had configured the value for this setting in the previous version of the application, and this value does not exceed 20,480 KB;
  - This setting has the default value of 1.536 KB (1.5 MB), if the administrator had not configured the value of this setting in the previous version of the application.
  - This setting has a value of 20,480 KB if its value in the previous version of the application exceeded 20,480 KB.
- Database structure will also be updated during the application update. Backup and statistical data will be preserved.

The current version of the application comes with a component called the DLP Module (see section "Data leak prevention" on page 99) that can be added to the existing configuration of the application during the upgrade. The DLP Module can be added if the Microsoft Exchange server is deployed in one of the following roles:

- Microsoft Exchange Server 2010 in the Hub Transport role
- Microsoft Exchange Server 2013 in the Mailbox role.

When upgrading the application on a Microsoft Exchange Server 2013 server deployed in the Mailbox role, the Anti-Virus module for the Mailbox role will be installed automatically.

Preparing to update

The application is updated using the Setup Wizard. During the update process, the Application Installation Wizard accesses the application database (see section "Backup and statistics database" on page 16). The account for which the update procedure is planned must have the following access rights:

- To the SQL server:
  - ALTER ANY LOGIN.
  - ALTER ANY CREDENTIAL.
- To the database:
  - CONNECT.
  - CREATE TYPE.
  - CREATE TABLE.
  - CREATE XML SCHEMA COLLECTION.

Before upgrading the application, you should also perform one of the following actions:

- Add the account under which you intend to perform the upgrade procedure, to the Domain Admins group
- Provide the Kse Watchdog Service group with the right to run under a different name (impersonation) by executing the following command in Exchange Management Shell console:

  ```
  New-ManagementRoleAssignment -Name KSE_IMPERSONATION -Role applicationImpersonation -SecurityGroup "Kse Watchdog Service"
  ```

Prior to updating, exit the Administration Console if it is started.
Application update procedure

To update the program to the current version, perform the following steps:

1. Run the setup.exe file included in the installation package on a computer with the installed version 9.0.

2. Click the link Kaspersky Security 9.0 for Microsoft Exchange Servers to initiate the application update process. A window with the text of the End User License Agreement opens.

3. Read and accept the terms of the End User License Agreement by selecting the I accept the terms of the License Agreement check box. Then click Next.

4. If the Microsoft Exchange server is deployed in a configuration suitable for installation of the DLP Module, the DLP Module Installation window opens. To add the DLP Module to the existing configuration of the application, select the Install DLP Module check box.

5. Click the Next button.

6. In the window that opens, click the Install button.

The Setup Wizard will perform subsequent application upgrade steps automatically.

7. When the application upgrade process finishes, click Finish to exit the application Setup Wizard.

All application components and modules installed on the computer are upgraded. The missing modules will be installed.

RESTORING THE APPLICATION

If the application encounters a failure while running (for example, if its executable files get damaged), you can restore the application using the Setup Wizard.

To restore Kaspersky Security:

1. Run the setup.exe file from the application installation package.

This opens the welcome window of the install package.

2. Click the Kaspersky Security 9.0 for Microsoft Exchange Servers link to open the welcome screen of the Setup Wizard and click Next.

3. In the Change, Restore or Remove the application window click the Restore button.

4. In the Restore window, click the Repair button.

This opens the Restore application window with information about restoring the application.

5. After the application has been restored, the Setup Wizard displays a notification about the completed application restoration. To finish restoring the application, click the Finish button.

During Kaspersky Security removal, services of MSExchangeTransport and MSExchangeIS will need a restart. Services will be restarted automatically without additional prompts.

Restoration of the application will not be possible if its configuration files are damaged. Removing and reinstalling the application is recommended in that case.

REMOVING THE APPLICATION

You can remove the application using the Setup Wizard or standard Microsoft Windows installation and removal tools. If the application is installed on several servers, it has to be removed from each server.

To remove Kaspersky Security from a computer, perform the following steps:

1. Run the setup.exe file from the application installation package.

This opens the welcome window of the install package.

2. Click the Kaspersky Security 9.0 for Microsoft Exchange Servers link to open the welcome screen of the Setup Wizard and click Next.
3. In the **Change, Restore or Remove the application** window click the **Remove** button.

4. In the **Remove** window, click the **Remove** button.
   This opens the **Remove application** window with information about application removal.

5. In the warning dialog that opens, perform the following operations:
   - If you want the application to save the database on the SQL server during application removal, click **Yes**.
     Backup data added by the application will be deleted from the database. Statistics data added by the application will be saved.
   - If you want the application to delete the database and statistics from the SQL server during application removal, click **No**.

6. After the application has been removed, the Setup Wizard displays a notification about the completed application removal. To finish removing the application, click the **Finish** button.

   During Kaspersky Security removal, services of MSExchangeTransport and MSExchangeIS will need a restart. Services will be restarted automatically without additional prompts.

   You can also uninstall the application using the standard software management tools in Microsoft Windows.
APPLICATION INTERFACE

The user interface of the application is provided by the Administration Console component. The Administration Console is a dedicated isolated snap-in integrated into Microsoft Management Console (MMC).

IN THIS SECTION:

Main window of the Administration Console ................................................................. 34
Administration Console tree .......................................................................................... 35
Workspace ..................................................................................................................... 35
Quick access pane ......................................................................................................... 35
Context menu .................................................................................................................. 36

MAIN WINDOW OF THE ADMINISTRATION CONSOLE

The main window of the Administration Console (see figure below) contains the following elements:

- **Menu**. Displayed immediately above the toolbar. The menu lets you manage files and windows and access the help system.
- **Toolbar**. Displayed in the upper part of the main window. The buttons on the toolbar allow direct access to some frequently accessed features of the application.
- **Administration Console tree**. Located in the left part of the main window. The Administration Console tree displays profiles, connected Security Servers, and Kaspersky Security settings. Profiles, connected Security Servers, and Kaspersky Security settings are displayed as nodes.
- **Workspace**. It is located in the right part of the main window. The workspace shows the contents of the node selected in the Administration Console tree.
- **Quick access bar**. It is located on the right from the workspace. The quick access bar lets you manage the selected node.

![Figure 3: Main application window](image-url)
CONSOLE TREE

The Administration Console tree shows the structure of profiles, Microsoft Exchange servers, and subnodes for managing application functions.

The Administration Console appears in the MMC tree with the Kaspersky Security 9.0 for Microsoft Exchange Servers root node. It contains the Profiles and <Server name> subnodes.

The Profiles node contains nodes with the names of all profiles created in the application. Such profiles appear as <Profile name> nodes. Each <Profile name> node contains the Servers node that shows subnodes with the names of Microsoft Exchange servers.

The DLP Module settings node is designed for DLP Module administration.

The <Server name> node is displayed for each protected Microsoft Exchange server to which the Administration Console is connected. As a result, the Administration Console tree can contain several nodes with Microsoft Exchange server names.

For every <Profile name> node, every <Server name> node, and every <Server name> subnode in the Servers node, the Administration Console tree shows the following subnodes designed for managing application functions:

- **Server protection**: manage e-mail traffic protection against malware and spam.
- **Updates**: manage database updates for the application.
- **Notifications**: configure settings pertaining to the application event notifications sent to the administrator and other persons concerned.
- **Backup**: configure Backup settings and manage objects stored there.
- **Reports**: configure application report settings (not shown for <Server name> subnodes in the Servers node).
- **Settings**: configure basic application settings.
- **Licensing** – view details of keys installed, install and remove keys.

WORKSPACE

The workspace shows information about the current Microsoft Exchange servers protection status, Kaspersky Security and application settings.

The appearance of the workspace depends on the node selected in the Administration Console tree.

QUICK ACCESS PANE

Specific links displayed in the quick access pane depend on the node selected in the Administration Console tree. Besides the standard links of the Microsoft Management Console, the quick access bar contains links for managing the selected node (see table below).

<table>
<thead>
<tr>
<th>NODE</th>
<th>LINK</th>
<th>LINK PURPOSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kaspersky Security 9.0 for Microsoft Exchange Servers</td>
<td>Connect to server</td>
<td>The Connect to server window opens.</td>
</tr>
<tr>
<td></td>
<td>Enable snap-in diagnostics</td>
<td>Starts keeping the Administration Console log.</td>
</tr>
<tr>
<td>Profiles</td>
<td>Add profile</td>
<td>Opens the Create new profile window.</td>
</tr>
<tr>
<td>&lt;profile name&gt;</td>
<td>Add server</td>
<td>Opens a wizard for adding the Security Server to the profile.</td>
</tr>
<tr>
<td></td>
<td>Rename</td>
<td>Opens the Rename profile window.</td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td>Removes the profile.</td>
</tr>
</tbody>
</table>
**CONTEXT MENU**

Each category of nodes in the Administration Console tree has its own context menu, which you can open by right-clicking.

Besides the standard items, the Microsoft Management Console context menu contains menu items for managing the selected node (see table below).

<table>
<thead>
<tr>
<th>NODE</th>
<th>MENU ITEM</th>
<th>PURPOSE OF THE MENU ITEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kaspersky Security 9.0 for Microsoft Exchange Servers</td>
<td>Connect to server</td>
<td>The Connect to server window opens.</td>
</tr>
<tr>
<td>Profiles</td>
<td>Add profile</td>
<td>Opens the Create new profile window.</td>
</tr>
<tr>
<td>Profiles</td>
<td>Enable snap-in diagnostics</td>
<td>Starts keeping the Administration Console log.</td>
</tr>
<tr>
<td>&lt;profile name&gt;</td>
<td>Add server</td>
<td>Opens a wizard for adding the Security Server to the profile.</td>
</tr>
<tr>
<td></td>
<td>Rename</td>
<td>Opens the Rename profile window.</td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td>Removes the profile.</td>
</tr>
<tr>
<td>Servers</td>
<td>Add server</td>
<td>Opens a wizard for adding the Security Server to the profile.</td>
</tr>
<tr>
<td>Profile → &lt;Security Server name&gt;</td>
<td>Remove from profile</td>
<td>Removes the Security Server from the profile.</td>
</tr>
<tr>
<td>Kaspersky Security 9.0 for Microsoft Exchange Servers → &lt;Security Server name&gt;</td>
<td>Remove server</td>
<td>Removes a Security Server from the Administration Console tree.</td>
</tr>
</tbody>
</table>
# APPLICATION LICENSING

This section provides information about general concepts related to the application licensing.

## In this section:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About the License Agreement</td>
<td>37</td>
</tr>
<tr>
<td>About the license</td>
<td>37</td>
</tr>
<tr>
<td>About the key file</td>
<td>38</td>
</tr>
<tr>
<td>About the license certificate</td>
<td>38</td>
</tr>
<tr>
<td>About the key</td>
<td>38</td>
</tr>
<tr>
<td>Types of keys used in the application</td>
<td>39</td>
</tr>
<tr>
<td>Licensing models</td>
<td>39</td>
</tr>
<tr>
<td>Special considerations of activating the application when using profiles</td>
<td>39</td>
</tr>
<tr>
<td>Special considerations of activating the application when using the key for the DLP Module</td>
<td>40</td>
</tr>
<tr>
<td>About notifications related to the license</td>
<td>40</td>
</tr>
<tr>
<td>About data submission</td>
<td>40</td>
</tr>
<tr>
<td>Activating the application</td>
<td>42</td>
</tr>
<tr>
<td>Viewing information about installed keys</td>
<td>43</td>
</tr>
<tr>
<td>Replacing a key</td>
<td>43</td>
</tr>
<tr>
<td>Removing a key</td>
<td>44</td>
</tr>
<tr>
<td>Configuring the license expiry term notification</td>
<td>45</td>
</tr>
</tbody>
</table>

## About the License Agreement

*The End User License Agreement* is a binding agreement between you and Kaspersky Lab ZAO, stipulating the terms on which you may use the application.

We recommend carefully reading the terms of the License Agreement before using the application.

You can view the terms of the License Agreement in the following ways:

- During installation of Kaspersky Security.
- By reading the license.txt file. This file is included in the application's distribution kit.

By confirming that you agree with the End User License Agreement when installing the application, you signify your acceptance of the terms of the End User License Agreement. If you do not accept the terms of the End User License Agreement, you must abort application installation and must not use the application.

## About the License

A *license* is a time-limited right to use the application, granted under the End User License Agreement.

A license entitles you to the following kinds of services:

- Use of the application in accordance with the terms of the End User License Agreement
- Technical support

The scope of services and application usage term depend on the type of license under which the application is activated.
The following license types are provided:

- **Trial** – a free license intended for trying out the application.
  A trial license is of limited duration. When the trial license expires, all Kaspersky Security features become disabled. To continue using the application, you need to purchase a commercial license.
  You can activate the application under a trial license only once.

- **Commercial** – a pay-for license that is provided when you buy the application.
  When the commercial license expires, the application continues running with limited functionality (for example, Kaspersky Security database updates are not available). To continue using Kaspersky Security in fully functional mode, you must renew your commercial license.

We recommend renewing the license before its expiration to ensure maximum protection of your computer against security threats.

**ABOUT THE KEY FILE**

A **key file** is a file with the .key extension that you receive from Kaspersky Lab. Key files are designed to activate the application by adding a key.

You receive a key file at the email address that you provided when you bought Kaspersky Security or ordered the trial version of Kaspersky Security.

You do not need to connect to Kaspersky Lab activation servers in order to activate the application with a key file.

You can recover a key file if it is accidentally deleted. You may need a key file to register with Kaspersky CompanyAccount.

To recover a key file, do one of the following:

- Contact Kaspersky Lab Technical Support ([https://companyaccount.kaspersky.com](https://companyaccount.kaspersky.com)).
- Obtain a key file on the Kaspersky Lab website ([https://activation.kaspersky.com](https://activation.kaspersky.com)) based on your existing activation code.

**ABOUT THE LICENSE CERTIFICATE**

The **License Certificate** is a document provided with the key file or activation code.

The License Certificate contains the following license information:

- Order ID;
- Details of the license holder
- Information about the application that can be activated using the license
- Limitation on the number of licensing units (devices on which the application can be used under the license)
- License start date
- License expiration date or license validity period
- License type

**ABOUT THE KEY**

A **key** is a sequence of bits with which you can activate and subsequently use the application in accordance with the terms of the End User License Agreement. A key is generated by Kaspersky Lab.

To add a key to the application, you have to apply a **key file**. After you add a key to the application, the key is displayed in the application interface as a unique alphanumeric sequence.

Kaspersky Lab can black-list a key over violations of the End User License Agreement. If the key has been black-listed, you have to add a different key to continue using the application.

A key may be an “active key” or an “additional key”. 
An active key is the key that is currently used by the application. A trial or commercial license key can be added as the active key. The application cannot have more than one active key.

An additional key is a key that entitles the user to use the application, but is not currently in use. An additional key automatically becomes active when the license associated with the current active key expires. An additional key may be added only if the active key is available.

A key for a trial license can be added only as the active key. A trial license key cannot be installed as the additional key.

**Types of keys used in the application**

For activating the application keys of the following types:

- **Security Server key.** Designed for using an application for protection of mail servers based on Microsoft Exchange Server against viruses, Trojan software and other types of threats that may be transmitted via e-mail, as well as spam and phishing.

- **DLP Module key.** Designed for using an application for protection from unintentional confidential data leaks from an organization by email.

**Licensing options**

Depending on the application deployment model (see section "Common application deployment models" on page 18), you have to add the following keys to activate the application (see section "Activating the application" on page 42):

- If the application is used on standalone Microsoft Exchange Servers, custom Security Server and DLP Module keys must be installed for each server.

- If the application is used on Microsoft Exchange Servers that are part of a DAG, it suffices to install a single Security Server key and a single DLP Module key that cover the entire DAG (see section "Application deployment in a Microsoft Exchange database availability group" on page 21).

- If you use profiles to manage several Security Servers, you have to add a single key of the Security Server and a single key of the DLP Module for the profile, that applies to all Security Servers (see section "Special considerations of activating the application when using profiles" on page 39).

If you do not use the DLP Module, you do not need to add the DLP keys.

**Special considerations of activating the application when using profiles**

If you use profiles (see section "About profiles" on page 58) to manage several Security Servers, make allowance for the following special considerations of activating the application:

- The effective term of the license is counted from the moment the active key is added. Active keys are automatically replaced with additional keys at the end of the effective term of the license on each of the Security Servers included in the profile, according to the time of the Microsoft Exchange server, on which the Security Server is installed. This is important when, for example, the Security Servers included in a profile are located in different time zones.

- In the Administration Console, in the workspace of the Profiles <profile name> \ Licensing node, the keys and license expiry dates are shown for each of the added keys according to the time of Administration Console. For example, if a license defined by the active key has expired according to the time of Administration Console and an additional key has been added, the workspace shows only the additional key and its properties.

- You cannot add, replace or delete a key separately for a Security Server that has been added to the profile. You can add, replace or delete a key only for all Security Servers in the profile, where the license applied to all Security Servers of the profile.

- After you have added a Security Server to a profile, the active key of this Security Server is replaced with the active key, added for the entire profile.

- After you have deleted the Security Server from the profile, the active key that was added for the profile is the one that remains active for the Security Server. The key for this Security Server is displayed in the workspace of the Licensing node.
SPECIAL CONSIDERATIONS OF ACTIVATING THE APPLICATION WHEN USING THE KEY FOR THE DLP MODULE

Special considerations of activating the application when using the key for the DLP Module are as follows:

- A DLP Module active key may be added only if there is an active key of the Security Server.
- A DLP Module additional key may be added only if there is a DLP Module active key and an additional key of the Security Server.
- The effective life of the active or additional keys of the DLP Module cannot exceed the effective life of the corresponding keys of the Security Server.
- When an active or additional key of the Security Server is deleted, the corresponding DLP Module key is also deleted.
- If the DLP Module active key is missing or its effective life has expired, the DLP Module shall operate in the following mode:
  - The DLP Module does not check messages for data leaks.
  - The Security Officer may work with DLP categories and DLP policies, incidents and reports (see Security Officer’s Guide to Kaspersky Security 9.0 for Microsoft Exchange Servers for detailed information).
  - DLP Module databases are updated together with the Anti-Virus databases.

ABOUT NOTIFICATIONS RELATED TO THE LICENSE

The application makes it possible to learn in good time about events and errors, related to the license, with the help of notifications.

The application draws up the following notifications related to the license:

- Notification on the blacklisting of a key.
  Sent after every update of the application databases on the Security Server, if the active key of the Security Server or the DLP Module key is blacklisted. Every Security Server to which a key is added that has been blacklisted sen its own notification. Different notifications are sent about a key of the Security Server or a key of the DLP Module being blacklisted.

- Notification about a pending license expiry.
  Sent once a day (at 00:00 hours UTC), if the aggregate effective term of the active and additional keys expires shall be reached in less than the set number of days (see the section "Configuring the license expiry notification" on page 45). By default, the application starts sending this notification 15 days before expiry of the aggregate effective term of the keys. Different notifications are sent about the pending end of the effective term of the key of the Security Server and the DLP Module key.

- Notification about an expired license.
  Sent once a day (at 00:00 hours UTC), if the aggregate effective term of the active key has ended and there is no additional key. Different notifications are sent about the expiry of the effective term of the key of the Security Server and the DLP Module key.

The application records these notifications in the log (see the section "Application logs" on page 111) and sends them by email if delivery of notifications about license-related events is enabled (see the section "Configuring notification settings" on page 102).

ABOUT DATA SUBMISSION

If you participate in Kaspersky Security Network (see section "About participation in Kaspersky Security Network" on page 72), you agree to send to Kaspersky Lab the following information pertaining to the operation of Kaspersky Security:

- Anti-Phishing requests:
  - Web address and IPv4/V6 address at which detection happened
  - ID of the application installation instance, application version
- Anti-Phishing databases release date and time
- Target of the attack
- Information from the Anti-Phishing module on the result of detection, including the trust level, weight, and status

- Anti-Spam requests:
  - IP address of the sender of the message that potentially contains spam
  - Hash (MD5, SHA1) of the address of the sender of the message that potentially contains spam
  - Web addresses contained in message with removed passwords that potentially contains spam
  - Check sums of graphic images in the message
  - MD5 hash of the name of the file attached to the message;
  - Technical information having to do with the method by which the application detected a message potentially containing spam;
  - Short text signatures (irreversible text conversions that do not make it possible to restore the original text; the text is not transmitted) for filtering out known spam campaigns and helping the application make decisions on them
  - Content filtering databases that have triggered, the text category (subject scope) defined by the application.

- Information transmitted to help detect new and hard-to-detect information security threats and their sources and intrusion threats, and raise the level of protection of information stored and processed:
  - Information about software installed on the computer, including the operating system version and service packs installed;
  - Details of the Kaspersky Lab application installed on the computer, including the name, version, and internal ID of installation of the application;
  - ID of the device on which the Kaspersky Lab application is installed;
  - Checksums of processed files (MD5);
  - Hash (SHA1) of the address of the sender and recipient of the message that potentially contains a threat or spam
  - Information about all potentially malicious objects and actions, including the name, size, hash (MD5) of the object detected, the date and time when the object was detected, the URL address and IP address from which the object was downloaded, information about object emulation, version of the Anti-Virus databases used, the ID of Anti-Virus databases based on which the application made the decision, and threat name according to the Kaspersky Lab classification.
  - Names of first-level domains from web addresses in messages being scanned
  - Code of the error that occurs when scanning the object, in case of a scanning error
  - Number of IP addresses of version 4 and version 6 in the header of the message being scanned.

- Information submitted to improve application performance:
  - Information about the version of the operating system and service packs installed on the computer
  - Version of the application component that performs the update, the ID of the update task type, application status after the update task, the code of the error that happened during the update process (if any)

No personal data of the user is collected, processed, or stored. Kaspersky Lab protects any information received in this way as prescribed by law and processes it anonymously.

The collected information is stored in encrypted form and destroyed as it is accumulated (twice per year). General statistics are stored indefinitely.

Participation in Kaspersky Security Network is voluntary. You can opt out of participating in the Kaspersky Security Network at any time (see section "Configuring spam and phishing scan settings" on page 84). You can also read the KSN Statement to find out about the types of data that the application relays to Kaspersky Security Network (see section "Configuring spam and phishing scan settings" on page 84).
ACTIVATING THE APPLICATION

If Kaspersky Security is installed in a configuration with a group of DAG servers, you only need to add one Security Server key and one DLP Module key for the entire DAG. You can install the key by connecting the Administration Console to any server within the DAG.

To activate the application, you need to add a key.

To add a key for a Security Server:
1. In the Administration Console tree open the node of the Security Server for which you wish to add a key.
2. Select the Licensing node.
3. In the workspace, perform one of the following actions:
   • To add the active key of the Security Server, click on the Add button in the Active Key section.
   • To add the additional key of the Security Server, click on the Add button in the Additional Key section.
   • To add the active key of the DLP Module, click on the Add button in the DLP Module Active Key section.
   • To add the additional key of the DLP Module, click on the Add button in the DLP Module Additional Key section.

   A DLP Module key may be added only if the active key of the Security Server is available.

   An additional key may be added only if the active key of the corresponding type is available.

   Only a commercial license key can be installed as the additional key. A trial license key cannot be installed as the additional key.

4. In the displayed File name dialog specify path to the key file (file with the .key extension) and click Open.

The key is added, and its details appear in the relevant section.

To add a key for a profile:
1. In the Administration Console tree, expand the Profiles node.
2. Expand the node of the profile for the Security Server of which you want to add the key.
3. Select the Licensing node.
4. In the workspace, perform one of the following actions:
   • To add the active key of the Security Server, click on the Add button in the Active Key section.
   • To add the additional key of the Security Server, click on the Add button in the Additional Key section.
   • To add the active key of the DLP Module, click on the Add button in the DLP Module Active Key section.
   • To add the additional key of the DLP Module, click on the Add button in the DLP Module Additional Key section.

   A DLP Module key may be added only if the active key of the Security Server is available.

   An additional key may be added only if the active key of the corresponding type is available.

   Only a commercial license key can be installed as the additional key. A trial license key cannot be installed as the additional key.

5. In the displayed File name dialog specify path to the key file (file with the .key extension) and click Open.

The key is added, and its details appear in the relevant section.
VIEWING INFORMATION ABOUT INSTALLED KEYS

To view the details of the installed keys:

1. Perform the following steps in the Administration Console tree:
   - To view the details of keys added for a Security Server, maximize the node of the Security Server the details of whose keys you want to view;
   - To view the details of keys added for a profile, maximize the Profiles node and inside it maximize the node of the profile the details of whose keys you want to view.

2. Select the Licensing node.

The workspace shows the following details about keys that have been added:

- **Status.** Possible values:
  - **Active license.** The license has not expired, and module functionality is not limited.
  - **Trial license validity period has expired.** The functionality of the modules is unavailable. The update of application databases is not allowed.
  - **License expired.** The license has expired, application database updates are unavailable, and access to KSN is blocked (see section “About additional services, features, and anti-spam technologies” on page 82).
  - **Databases corrupted.** The application databases are missing or damaged.
  - **Key is missing.** The functionality of the modules is unavailable. The update of application databases is not allowed.
  - **Key blocked.** Only application database updates are available. The functionality of the modules is unavailable.
  - **Key blacklist corrupted or missing.** Only application database updates are available. The functionality of the modules is unavailable.

   This field is displayed only for active keys.

- **Key.** Unique alphanumeric sequence.
- **License type.** License type (Trial, Commercial).
- **Representative.** Contact person of the organization that signed the End User License Agreement.
- **Number of users.** The maximum number of application users whose mailboxes can be protected by the application with this key.
- **Expiration date.** License expiration date.

REPLACING A KEY

To replace a key added for a Security Server:

1. In the Administration Console tree open the node of the Security Server for which you wish to add a key.
2. Select the Licensing node.
3. In the workspace, perform one of the following actions:
   - To replace the active key of the Security Server, click on the Replace button in the Active Key section.
   - To replace the additional key of the Security Server, click on the Replace button in the Additional Key section.
   - To replace the active key of the DLP Module, click on the Replace button in the DLP Module Active Key section.
   - To replace the additional key of the DLP Module, click on the Replace button in the DLP Module Additional Key section.
4. In the displayed File name dialog specify path to the key file (file with the .key extension) and click Open.

The key is replaced, and details about the new key appear in the relevant section.
To replace a key added for a profile:
1. In the Administration Console tree, expand the Profiles node.
2. Expand the node of the profile whose key you want to replace.
3. Select the Licensing node.
4. In the workspace, perform one of the following actions:
   - To replace the active key of the Security Server, click on the Replace button in the Active Key section.
   - To replace the additional key of the Security Server, click on the Replace button in the Additional Key section.
   - To replace the active key of the DLP Module, click on the Replace button in the DLP Module Active Key section.
   - To replace the additional key of the DLP Module, click on the Replace button in the DLP Module Additional Key section.
5. In the displayed File name dialog specify path to the key file (file with the .key extension) and click Open.
   The key is replaced, and details about the new key appear in the relevant section.

REMOVING A KEY

To remove a key added for a Security Server:
1. In the Administration Console tree open the node of the Security Server for which you wish to remove a key.
2. Select the Licensing node.
3. In the workspace, perform one of the following actions:
   - To delete the active key of the Security Server, click on the Delete button in the Active Key section.
   - To delete an additional key of the Security Server, click on the Delete button in the Additional Key section.
   - To delete the active key of the DLP Module, click on the Delete button in the DLP Module Active Key section.
   - To delete the additional key of the DLP Module, click on the Delete button in the DLP Module Additional Key section.
   The application deletes the selected key. When the active key is deleted, the additional key (if installed) becomes active.

To delete a key added for a profile:
1. In the Administration Console tree, expand the Profiles node.
2. Expand the node of the profile whose key you want to remove.
3. Select the Licensing node.
4. In the workspace, perform one of the following actions:
   - To delete the active key of the Security Server, click on the Delete button in the Active Key section.
   - To delete an additional key of the Security Server, click on the Delete button in the Additional Key section.
   - To delete the active key of the DLP Module, click on the Delete button in the DLP Module Active Key section.
   - To delete the additional key of the DLP Module, click on the Delete button in the DLP Module Additional Key section.
   The application deletes the selected key. When the active key is deleted, the additional key (if installed) becomes active.
CONFIGURING THE LICENSE EXPIRY TERM NOTIFICATION

To configure Security Server license expiry term notifications:

1. In the Administration Console tree, expand the node of the Security Server you need.
2. Select the Notifications node.
3. In the lower part of the details pane, in the spin box of the Notify about license expiry in setting, specify in how many days before license expiry you want to receive a notification about license expiry.
   
   Notifications are sent only if the check box Notify about events related to the license is enabled. Notifications are sent to the e-mail addresses, specified below in this section.
4. Click the Save button.

To configure profile license expiry term notifications:

1. In the Administration Console tree, expand the Profiles node.
2. Expand the node of the profile for whose Security Servers you want to configure license expiry notifications.
3. Select the Notifications node.
4. In the lower part of the details pane, in the spin box of the Notify about license expiry in setting, specify in how many days before license expiry you want to receive a notification about license expiry.
   
   Notifications are sent only if the check box Notify about events related to the license is enabled. Notifications are sent to the e-mail addresses, specified below in this section.
5. Click the Save button.
STARTING AND STOPPING THE APPLICATION

This section contains information on starting and shutting down the application.

In this section:

Starting and stopping a Security Server ................................................................. 46
Starting: Administration Console ............................................................................. 46
Adding Security Servers to Administration Console ............................................... 47

STARTING AND STOPPING A SECURITY SERVER

A Security Server starts automatically in the following cases:

- After the application installation
- When running the operating system on a computer with an installed Security Server, if the Automatic run mode has been selected in the settings of Kaspersky Security for Microsoft Exchange Servers.

You can run and stop a Security Server manually.

To stop a Security Server manually:

1. In the Administration Console, disable anti-virus protection (see section "Enabling and disabling anti-virus protection of the server" on page 72) and anti-spam protection (see section "Enabling and disabling anti-spam protection of the server" on page 83 on the Security Server).
2. On the computer hosting the Security Server, use the tools of the operating system to stop the Kaspersky Security for Microsoft Exchange Servers service and change its launch type to Disabled.

To run a Security Server manually:

1. On the computer hosting the Security Server, use the operating system’s tools to run Kaspersky Security for Microsoft Exchange Servers and set its run mode to Automatic.
2. In Administration Console, enable the anti-virus protection (see the section "Enabling and disabling the anti-virus protection of a server" on page 72) and the anti-spam protection (see the section "Enabling and disabling the anti-spam protection of a server" on page 83).

STARTING THE ADMINISTRATION CONSOLE

Before starting Administration Console, make sure your account is assigned the Administrator role (see the section "Role-based access" on page 56).

To launch the Administration Console,


When the Administration Console starts, the Kaspersky Security snap-in connects to MMC, and the Administration Console tree displays the application icon and the Kaspersky Security 9.0 for Microsoft Exchange Servers node.

When Administration Console is running, you can add the Microsoft Exchange servers with an installed Security Server (hereinafter referred to as protected servers) to Administration Console.

The application records information about starts and stops of Administration Console to Windows Event Log. Each record contains information about the start / stop time of Administration Console, as well as the user who initiated those actions.
To allow managing the application, the protected servers must be added to Administration Console.

If the Security Servers are installed on Microsoft Exchange servers included in a Microsoft Exchange database availability group (DAG), you can connect Administration Console to any of those Security Servers in order to define the settings shared by the entire DAG, or connect Administration Console to an individual Security Server in order to define its own settings.

Shared settings of the entire DAG include, e.g., the anti-virus protection settings for the Mailbox role, the Anti-Virus reporting settings for the Mailbox role, the notification settings, and the update settings of Anti-Virus databases. The entire DAG also shares the contents of Backup and the key.

Examples of individual settings of the Microsoft Exchange Server include: anti-virus protection settings for the Hub Transport role, anti-spam scan settings, Backup settings, settings of the Anti-Spam and Anti-Virus reports for the Hub Transport role, and Anti-Spam database update settings.

To add a Security Server to Administration Console:

1. Select the Kaspersky Security 9.0 for Microsoft Exchange Servers node in the Administration Console tree.

2. Open the Add server window in one of the following ways:
   - By selecting the Add server item in the Action menu.
   - By selecting the Add server item in the context menu of the Kaspersky Security 9.0 for Microsoft Exchange Servers node.
   - By clicking the Add server button in the workspace of the node.
   - By clicking the Add server link in the quick access pane.

3. In the Add server window, select the Security Server deployed on the Microsoft Exchange server, to which you want to connect the Administration Console:
   - If you want to connect the Administration Console to a Security Server deployed on a local computer, choose the Local option.
   - If you want to connect the Administration Console to a Security Server deployed on a remote Microsoft Exchange Server, choose the Remote option.

   Administration Console connects to the Security Server via TCP port 13100. You have to open this port in the firewall on the remote Microsoft Exchange server or add the service of Kaspersky Security 9.0 for Microsoft Exchange Servers to the list of trusted applications of the firewall.

4. If you have chosen the Remote option, in the entry field specify the name of the remote Microsoft Exchange Server on which the Security Server is deployed. You can select the remote Microsoft Exchange server from the list by clicking the Browse button or by typing manually one of the values for the remote Microsoft Exchange server:
   - IP address
   - Fully-qualified domain name (FQDN) in the format <Computer name>.<DNS-domain name>
   - Computer name on the Microsoft Windows network (NetBIOS name)

5. Click OK.

   The added Security Server appears in the Administration Console tree.

The Security Servers that have been added are displayed in the Administration Console tree as separate nodes. To proceed to the management of a Security Server, you should expand the corresponding node.

You can also manage a group of Security Servers by means of profiles (see the section "Managing profiles" on page 58).
SERVER PROTECTION STATUS

This section covers the default settings of Kaspersky Security. This section describes how you can use the Administration Console to view license info, the status of application modules and databases, as well as statistics on the number of messages processed and instances of threats and spam detected.

**IN THIS SECTION:**

Default Microsoft Exchange Server protection ................................................................................................................. 48
Viewing Microsoft Exchange Server protection status details .......................................................................................... 49
Viewing profile protection status details ........................................................................................................................... 53

**DEFAULT MICROSOFT EXCHANGE SERVER PROTECTION**

Anti-virus and anti-spam protection of the Microsoft Exchange server starts immediately after the Security Server component is installed unless it has been turned off in the Application Configuration Wizard (see section "Step 2. Configuring server protection" on page 29).

The following application mode is engaged by default:

- The application scans messages for all currently known malware in Anti-Virus databases with the following settings:
  - The application scans the message body and attached objects in any format, except for container objects with a nesting level above 32.
  - The application scans all storages of public folders and all mailbox storages.
  - The choice of the operation performed upon detection of an infected object depends on the role of the Microsoft Exchange Server where the object has been detected:
    - When an infected object is detected on a Microsoft Exchange Server in a Hub Transport or Edge Transport role, the object is deleted automatically, and the application saves the original copy of the message in Backup and adds the [Malicious object deleted] tag to the message subject.
    - When an infected object is detected on a Microsoft Exchange Server in a Mailbox role, the application saves the original copy of the object (attachment or message body) in Backup and attempts disinfection. If disinfection fails, the application deletes the object and replaces it with a text file containing the following notification:
      
      Malicious object <VIRUS_NAME> has been detected. The file (<object_name>) was deleted by Kaspersky Security 9.0 for Microsoft Exchange Servers. Server name: <server_name>

- When a password-protected or corrupted object is detected, the application skips it.

- The application scans messages for spam with the following settings:
  - The application uses the low sensitivity level of anti-spam scanning. This level provides an optimal combination of scanning speed and quality.
  - The application skips all messages. Messages that have been labeled as Spam, Probable spam, Mass mailing, or Blacklisted are marked with special tags in the message subject: [!!SPAM], [!!Probable Spam], [!!Mass Mail] and [!!Blacklisted], respectively.
  - The maximum duration for scanning a single message is 60 seconds.
  - The maximum size of a message with attachments to be scanned is 1,536 KB (1.5 MB).
  - External services are used to check IP addresses and URLs: DNSBL and SURBL (see section "About additional services, features, and anti-spam technologies" on page 82). These services enable spam filtering using public black lists of IP addresses and URLs.
If you have enabled the use of KSN in the Application Configuration Wizard (see the section "Step 3. Enabling the KSN service" on page 29), the use of KSN and Reputation Filtering services is enabled. Otherwise, the KSN and Reputation Filtering services are disabled.

If you have enabled the use of Enforced Anti-Spam Updates Service in the Application Configuration Wizard (see the section "Step 2. Configuring server protection" on page 29), the use of Enforced Anti-Spam Updates Service is enabled. Otherwise, the use of the Enforced Anti-Spam Updates Service is disabled.

The application does not scan outgoing messages for data leaks (see section "Data Leak Prevention" on page 99). If the DLP Module is installed, you should configure the DLP policies (see Security Officer’s Guide to Kaspersky Security 9.0 for Microsoft Exchange Servers for detailed information).

If you have enabled the feature of application databases updating in the Application Configuration Wizard (see the section "Step 2. Configuring server protection" on page 29), the databases are updated regularly from Kaspersky Lab update servers (with the frequency of once per hour for Anti-Virus and DLP Module databases, once every five minutes for Anti-Spam databases).

**VIEWING MICROSOFT EXCHANGE SERVER PROTECTION STATUS DETAILS**

To Microsoft Exchange Server protection status details:


2. In the Administration Console tree, select the node of the Security Server installed on the relevant Microsoft Exchange server whose status you want to view.

The workspace of the selected Security Server node shows the following information about the status of server protection:

- **The Profile** section explains how to configure Security Server settings by means of profiles.
- **The Product info** section shows information about the Microsoft Exchange server and the application modules:
  - **Server name.**
    - The server name can take the following values:
      - Name of the physical server if the Administration Console is connected to a Security Server deployed on a standalone Microsoft Exchange server, a passive node within a cluster, or on a server that belongs to a DAG.
      - Virtual server name, if the Administration Console is connected to a virtual server or its active node.
  - **Details of the application deployment model.**
    - The field contains one of the following values:
      - Virtual Server, if the Administration Console is connected to a virtual Microsoft Exchange Server or its active node.
      - «DAG name>, if the Administration Console is connected to a Security Server deployed on a Microsoft Exchange server that belongs to a DAG.
  - **Version.**
    - Details of the application version.
  - **Anti-Spam module.**
    - Status of the Anti-Spam module. Shown if the Microsoft Exchange Server is deployed as a Hub Transport or Edge Transport. Possible values:
      - Disabled – the Anti-Spam module is installed, anti-spam scanning of messages is disabled.
      - Not active – the Anti-Spam module is installed, anti-spam scanning of messages is enabled, but the Anti-Spam module is not scanning messages for spam due to licensing errors, Anti-Spam database errors, or scan errors.
      - Not installed: the Anti-Spam module is not installed.
      - Enabled – the Anti-Spam module is installed, and anti-spam scanning of messages is enabled.
- **Anti-Virus module for Hub Transport role.**
  Status of the Anti-Virus module for the Hub Transport role. Shown if the Microsoft Exchange Server is deployed as a Hub Transport or Edge Transport. Possible values:
  - **Disabled** – the Anti-Virus module is installed for the Hub Transport and Edge Transport roles, and anti-virus protection for the Hub Transport role is disabled.
  - **Not active** – the Anti-Virus module is installed for the Hub Transport and Edge Transport roles, anti-virus protection for the Hub Transport role is enabled, but the Anti-Virus module is not scanning messages for viruses and other threats due to licensing errors, database errors, or scan errors.
  - **Not installed** – the Anti-Virus module is not installed for the Hub Transport and Edge Transport roles.
  - **Enabled** – the Anti-Virus module is installed for the Hub Transport and Edge Transport roles, anti-virus protection for the Hub Transport role is enabled, and the Anti-Virus module scans messages for viruses and other threats.

- **Anti-Virus module for Mailbox role.**
  Status of the Anti-Virus module for the Mailbox role. Shown if the Microsoft Exchange Server is deployed in Mailbox role. Possible values:
  - **Disabled** – the Anti-Virus module is installed for the Mailbox role, and the anti-virus protection for the Mailbox role is disabled.
  - **Does not work** – the anti-virus protection is enabled for the Mailbox role, but the Anti-Virus module does not scan messages for viruses and other threats due to licensing errors, database errors, or scan errors.
  - **Not installed** – the Anti-Virus module is not installed for the Mailbox role.
  - **Enabled** – the anti-virus protection is enabled for the Mailbox role, and the Anti-Virus module scans messages for viruses and other threats.

- **DLP Module.**
  DLP Module status. Possible values:
  - **Disabled** – the DLP Module is installed, but it is disabled.
  - **Not active** – the DLP Module is installed and enabled, but it is not scanning messages for data leaks due to licensing errors, database errors, or scan errors.
  - **Not installed** – the DLP Module is not installed.
  - **Enabled** – the DLP Module is installed and enabled.

The set of fields reflecting the state of Security Server modules may be shorter, depending on the configuration of the Microsoft Exchange Server. If the field corresponding to a module is not displayed, this module cannot be installed with the current configuration of the Microsoft Exchange Server.

If the SQL server is unavailable, the **Product info** configuration section shows information about an SQL server connection error.

Clicking the **Go to server protection settings** link opens the workspace of the **Server protection** node.

- **The Licensing and DLP Licensing** section shows information about the current license:
  - **Functionality.**
    Available application features determined by the current license. Possible values:
    - **Full functionality.**
    - **License expired. Database updates and technical support are unavailable.**
    - **Management only.**
    - **Update only.**
  - **Status.**
    License status for Anti-Virus and Anti-Spam can take the following values:
    - **Active license.** The functionality of Anti-Virus and Anti-Spam is unlimited.
    - **Trial license validity period has expired.** The functionality of the Anti-Virus and Anti-Spam modules is unavailable. Updates are not allowed.
    - **License expired.** Updates are blocked, Kaspersky Security Network is unavailable.
    - **Databases corrupted.** Anti-Virus or Anti-Spam databases are corrupted or missing.
• **Key is missing.** The functionality of the Anti-Virus and Anti-Spam modules is unavailable. Updates are not allowed.

• **Key blocked.** Only database updates are available. The functionality of the Anti-Virus and Anti-Spam modules is unavailable.

• **Key blacklist corrupted or missing.** Only database updates are available. The functionality of the Anti-Virus and Anti-Spam modules is unavailable.

License status for the DLP Module can take the following values:

• **Active license.** DLP Module functionality is unlimited.

• **Trial license validity period has expired.** The functionality of the DLP Module is unavailable. The update is not allowed.

• **License expired.** Updates are blocked, Kaspersky Security Network is unavailable.

• **Databases corrupted.** The DLP Module databases are missing or damaged.

• **Key is missing.** The functionality of the DLP Module is unavailable. The update is not allowed.

• **Key blocked.** Only database updates are available. The functionality of the DLP Module is unavailable.

• **Key blacklist corrupted or missing.** Only database updates are available. The functionality of the DLP Module is unavailable.

If a value is displayed in the **Status** field of the Licensing or DLP Licensing sections, which differs from Effective license, the respective section is highlighted in red. This requires installing an appropriate active key (see section "Activating the application" on page 42) after opening the Licensing section via the Manage keys link.

• **Expiration date.**

  License expiration date.

  If the **Expiration date** field is highlighted in red, you have to renew the license, for example by adding an appropriate additional key (see section "Activating the application" on page 42) by opening the Licensing node via the Manage keys link.

The time period until the license expiration during which the field is highlighted in red is defined by the Notify N days before license expiry setting (see the section "Configuring the license expiry notification" on page 45) located in the workspace of the Notifications node. The default value is 15 days.

• **Number of users.**

  The maximum number of users whose mailboxes can be protected by the application with this key.

• **Additional key.**

  Information on the availability of an additional key: Added or Not found.

  Clicking the Manage keys link opens the workspace of the Licensing node in which you can add or remove keys.

  The DLP Licensing section displays only if the DLP Module is installed on the Security Server.

• **The Anti-Spam database section** shows the following Anti-Spam database status information:

  • **Last update.**

    Date of the last update of the Anti-Spam databases.

  • **Status.**

    Status of the last update of the Anti-Spam databases. Possible values:

    • **Database updated** – database update was successful.

    • **Completed with an error** – an error was encountered while updating the database.

    • **Not performed** – the database update task was not performed.

  • **Release date and time.**

    Anti-Spam database release date and time. Displayed in the date format defined in the settings of the operating system.

    If the Anti-Spam databases are outdated by more than one hour, the text in this field is highlighted in red.
If the Anti-Spam database section or the Release date and time field within this section are highlighted in red, update the Anti-Spam databases (see section "Updating databases manually" on page 64). If necessary, you can configure Anti-Spam database update settings (see section "Configuring scheduled database updates" on page 65).

If the last Anti-Spam database update ended in an error, the Anti-Spam databases section is highlighted in red and the error message is displayed in the Status field.

Clicking the Configure update settings link opens the workspace of the Updates node.

- The Anti-Virus and DLP Module databases section shows information about the status of the Anti-Virus and DLP Module databases:
  - Last update.
    The date of the last Anti-Virus and DLP Module database update.
  - Status.
    The status of the last Anti-Virus and DLP Module database update. Possible values:
    - Database updated – database update was successful.
    - Completed with an error – an error was encountered while updating the database.
    - Not performed – the database update task was not performed.
  - Release date and time.
    The date and time of the release of the Anti-Virus and DLP Module databases. Displayed in the date format defined in the settings of the operating system.
    If the Anti-Virus and DLP Module databases are outdated by more than one day, the text in this field is highlighted in red.
  - Records in the base.
    Number of records describing known threats and stored in the Anti-Virus database.

If the Databases of Anti-Virus and DLP Module section or the Release date and time field within this section is highlighted in red, update the Anti-Virus and DLP Module databases (see section "Updating databases manually" on page 64). If necessary, you can configure Anti-Virus and DLP Module database update settings (see section "Configuring scheduled database updates" on page 65).

If the last Anti-Virus and DLP Module database update ended in an error, the Anti-Virus and DLP Module databases section is highlighted in red and the error message is displayed in the Status field.

Clicking the Configure update settings link opens the workspace of the Updates node.

- The Statistics section shows the following counters with the number of messages moved to Quarantine for rescanning for spam (see page 80):
  - Total number of messages moved to Quarantine by the application.
    Number of messages moved to Quarantine since the application started tracking statistics.
  - Number of messages in Quarantine.
    Number of messages currently in Quarantine.

Charts with performance statistics of application modules over the past seven days are displayed under the counters in the Statistics section:

- Anti-Spam.
  The chart includes the following information:
  - Total messages. Number of processed messages.
  - With phishing or spam. Number of scanned messages containing phishing links or spam.
  - Unscanned. Number of messages left unchecked.
  - Clean. Number of scanned messages without phishing links or spam.
  - Other items. Number of messages belonging to the following categories:
    - Potential spam.
    - Formal notification.
    - Mass mail.
• Message matching black or white list criteria.
• Messages coming over authorized connections (if checking of authorized connections has been disabled).

• **Anti-Virus for Hub Transport role.**

The chart includes the following information:
• **Total messages.** Number of processed messages.
• **Infected.** Number of infected messages detected.
• **Unscanned.** Number of messages left unchecked.
• **Uninfected.** Number of checked messages that are free from threats.
• **Other items.** Number of messages belonging to the following categories:
  • Probably infected.
  • Protected.
  • Corrupted.

• **Anti-Virus for the Mailbox role.**

The chart includes the following information:
• **Server name.** Name of the connected server.
• **Total messages.** Number of processed messages.
• **Infected.** Number of infected messages detected.
• **Unscanned.** Number of messages left unchecked.
• **Uninfected.** Number of checked messages that are free from threats.
• **Other items.** Number of messages belonging to the following categories:
  • Probably infected.
  • Protected.
  • Corrupted.

The set of charts may be abbreviated depending on the configuration of the application.

Clicking the **Go to reports** link opens the workspace of the **Reports** node in which you can generate application reports.

**VIEWING PROFILE PROTECTION STATUS DETAILS**

1. Start Administration Console by going to the **Start** menu of the operating system and selecting **Programs → Kaspersky Security 9.0 for Microsoft Exchange Servers → Kaspersky Security 9.0 for Microsoft Exchange Servers.**

2. In the **Profiles** node of the Administration Console tree, select the node of the profile whose protection status details you want to view.

The following information appears in the workspace of the selected profile:

• **Functionality.**

  Available application features determined by the current license. Possible values:
  • Full functionality.
  • License expired. Database updates and technical support are unavailable.
  • Management only.
  • Update only.
• **Status.**

License status for Anti-Virus and Anti-Spam can take the following values:

- **Active license.** The functionality of Anti-Virus and Anti-Spam is unlimited.
- **Trial license validity period has expired.** The functionality of the Anti-Virus and Anti-Spam modules is unavailable. Updates are not allowed.
- **License expired.** Updates are blocked, Kaspersky Security Network is unavailable.
- **Databases corrupted.** Anti-Virus or Anti-Spam databases are corrupted or missing.
- **Key is missing.** The functionality of the Anti-Virus and Anti-Spam modules is unavailable. Updates are not allowed.
- **Key blocked.** Only database updates are available. The functionality of the Anti-Virus and Anti-Spam modules is unavailable.
- **Key blacklist corrupted or missing.** Only database updates are available. The functionality of the Anti-Virus and Anti-Spam modules is unavailable.

License status for the DLP Module can take the following values:

- **Active license.** DLP Module functionality is unlimited.
- **Trial license validity period has expired.** The functionality of the DLP Module is unavailable. The update is not allowed.
- **License expired.** Updates are blocked, Kaspersky Security Network is unavailable.
- **Databases corrupted.** The DLP Module databases are missing or damaged.
- **Key is missing.** The functionality of the DLP Module is unavailable. The update is not allowed.
- **Key blocked.** Only database updates are available. The functionality of the DLP Module is unavailable.
- **Key blacklist corrupted or missing.** Only database updates are available. The functionality of the DLP Module is unavailable.

If the Status field shows a value other than **Active license**, the Licensing section is highlighted in red. This requires installing an active key (see section "Activating the application" on page 42) after opening the Licensing section via the Manage keys link.

• **Expiration date.**

License expiration date.

If the Expiration date field is highlighted in red, you have to renew the license, for example by adding an additional key (see section "Activating the application" on page 42) by opening the Licensing node via the Manage keys link.

The period of time until license expiry during which the field is highlighted in red is defined by the Notify N days before license expiry setting (see the section "Configuring the notification about license expiry" on page 45). This setting is located in the workspace of the Licensing node. The default value is 15 days.

• **Number of users.**

The maximum number of users whose mailboxes can be protected by the application with this key.

• **Additional key.**

Information on the availability of an additional key: **Added** or **Not found**.

Clicking the Manage keys link opens the workspace of the Licensing node in which you can add or remove keys.

• **The Server state section** shows a table whose columns contain information about the state of profile servers, updates, application modules, and the SQL server:

- **Server.**

The server name can take the following values:

- **<Server domain name>,** if the profile includes a Security Server deployed on a Microsoft Exchange server that does not belong to a DAG and is not a passive node within a cluster.
- **<DAG name – Server domain name>,** if the profile includes a Security Server deployed on a Microsoft Exchange server that belongs to a DAG.
- **<Virtual server name – Server domain name>,** if the profile includes a virtual server.
• **Update status.**

Status of database updates on the server. Possible values:

- **Database updated** – databases have been successfully updated;
- **Database error** – there has been an error during database updates, databases are obsolete or corrupted, or no updates have been performed;
- **Server unavailable** – the server is unavailable on the network or turned off.

• **Anti-Virus module.**

Status of the Anti-Virus module. Possible values:

- **Disabled** – the Anti-Virus module for the Hub Transport and Edge Transport roles or the Anti-Virus module for the Mailbox role is installed; anti-virus scanning of messages is disabled.
- **Not active** – the Anti-Virus module for the Hub Transport and Edge Transport roles or the Anti-Virus module for the Mailbox role is installed; anti-virus scanning of messages is enabled, but the Anti-Virus module cannot scan messages for viruses and other threats due to licensing errors, database errors, or scan errors.
- **Not installed** – the Anti-Virus module is not installed for the Hub Transport and Edge Transport roles or the Mailbox role.
- **Enabled** – the Anti-Virus module for the Hub Transport and Edge Transport roles or the Anti-Virus module for the Mailbox role is installed; anti-virus scanning of messages is enabled; the Anti-Virus module scans messages for viruses and other threats.

• **Anti-Spam module.**

Status of the Anti-Spam module. Shown if the Microsoft Exchange Server is deployed as a Hub Transport or Edge Transport. Possible values:

- **Disabled** – the Anti-Spam module is installed, anti-spam scanning of messages is disabled.
- **Not active** – the Anti-Spam module is installed, anti-spam scanning of messages is enabled, but the Anti-Spam module is not scanning messages for spam due to licensing errors, Anti-Spam database errors, or scan errors.
- **Not installed** – the Anti-Spam module is not installed.
- **Enabled** – the Anti-Spam module is installed, and anti-spam scanning of messages is enabled.

• **DLP Module.**

DLP Module status. Possible values:

- **Disabled** – the DLP Module is installed, but it is disabled.
- **Not active** – the DLP Module is installed and enabled, but it is not scanning messages for data leaks due to licensing errors, database errors, or scan errors.
- **Not installed** – the DLP Module is not installed.
- **Enabled** – the DLP Module is installed and enabled.

• **SQL server.**

The status of the SQL server. Possible values:

- **Available.**
- **Unavailable.**

If the Security Server is unavailable, the **Update status** column shows the **Server unavailable** status, and the **Update status**, **Anti-Virus module**, **Anti-Spam module**, and **DLP Module** columns are highlighted in red.

If the **Update status** column shows a value other than **Databases are up to date**, the column is highlighted in red.

If the status of the Anti-Virus, Anti-Spam of DLP modules is **Disabled** or **Does not work**, the column corresponding to the module is highlighted in red.

Clicking the server name in the **Server** column opens the workspace of the server node.
ROLE-BASED ACCESS

Kaspersky Security contains facilities for role-based access to application functions.

Roles of application users

Kaspersky Security 9.0 for Microsoft Exchange Servers supports two-role scenario of user access to the application. Each role is assigned a set of available application functions and, accordingly, a set of available nodes displayed in the Administration Console tree. The functions of roles do not overlap.

Application users can be assigned the following roles:

- **Administrator.** A professional performing general application administration tasks, such as configuring Anti-Virus and Anti-Spam settings or creating Anti-Virus and Anti-Spam operation reports. This document describes the administrator tasks and instructions on performing them.

- **Security officer** A specialist tasked with administering confidential data leak prevention tools (the DLP Module): configuring DLP categories and policies, processing incidents. The tasks of the security officer and instructions on performing them are provided in the Security Officer’s Guide.

The table below shows the roles and the corresponding sets of nodes that are displayed in the Administration Console tree.

<table>
<thead>
<tr>
<th>ROLE</th>
<th>NODES DISPLAYED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>• Profiles.</td>
</tr>
<tr>
<td></td>
<td>• DLP module settings.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;Security Server name&gt;</code>.</td>
</tr>
<tr>
<td></td>
<td>• Server protection.</td>
</tr>
<tr>
<td></td>
<td>• Updates.</td>
</tr>
<tr>
<td></td>
<td>• Notifications.</td>
</tr>
<tr>
<td></td>
<td>• Backup.</td>
</tr>
<tr>
<td></td>
<td>• Reports.</td>
</tr>
<tr>
<td></td>
<td>• Settings.</td>
</tr>
<tr>
<td></td>
<td>• Licensing.</td>
</tr>
<tr>
<td>Security Officer</td>
<td>• Data Leak Prevention.</td>
</tr>
<tr>
<td></td>
<td>• Reports.</td>
</tr>
<tr>
<td></td>
<td>• Categories and policies.</td>
</tr>
<tr>
<td></td>
<td>• Incidents.</td>
</tr>
</tbody>
</table>

Roles are assigned by adding a user account to one of the following Active Directory groups:

- Kse Administrators (for administrators).
- Kse Security Officers (for security officers).

These groups are created automatically when the application is installed or upgraded to Kaspersky Security 9.0 for Microsoft Exchange Servers. Groups can be also created manually prior to installation of the application using standard Active Directory data management tools. Groups can be created in any domain of the organization. The type of groups is “Universal”.

When Administration Console is launched, the application checks which group includes the user account under which Administration Console has been launched, and the user's role in the application is determined on the basis of this information.
If a user needs to combine both roles and manage all functions of Kaspersky Security, the user's account should be added to both Active Directory groups.

**System role**

In addition to the user roles in the application there is also a system role. A system role will be held by the account on behalf of which the Kaspersky Security 9.0 for Microsoft Exchange Servers application service will be launched.

The system role is assigned by the account you select during application installation. If after application installation you want to specify another account for launching the application service, you should assign it a system role. To assign a system role to an account, add it to the Active Directory group with the name Kse Watchdog Service.
MANAGING PROFILES

This section describes how you can create, manage, and configure profiles.

IN THIS SECTION:

About profiles .......................................................... 58
Creating a profile ...................................................... 59
Configuring Security Servers in a profile ......................... 59
Specifics of managing profiles in a Microsoft Exchange database availability group ..................... 60
Adding Security Servers to a profile .............................. 60
Removing a Security Server from a profile ....................... 61
Removing a profile .................................................... 62

ABOUT PROFILES

If a corporate network includes several Microsoft Exchange servers with the application installed, you may need to manage the application settings in a group of servers simultaneously. For example, these may be Microsoft Exchange servers with identical security requirements. To manage identical settings in a group of Security Servers, Kaspersky Security provides profiles. A profile is a set of identical settings applied to several Security Servers at once. Using profiles allows you to specify identical settings for all Security Servers of the same type simultaneously and to avoid the hassle of configuring each Security Server separately.

Profiles can be useful in the following cases:

- There are several Microsoft Exchange servers with the application on the corporate network and you need to manage these servers in the same way. In this case, you can create a single profile, add all Security Servers to this profile, and configure application settings in the profile.

- There are two or more groups of Security Servers on the corporate network, and you need to configure different settings for these groups. In this case, the following profile usage options are possible:
  - If each of the groups includes more than one Security Server, you can create several profiles with different settings and add different Security Servers to them.
  - If one of the Security Servers requires custom settings, you can create a profile for a group of servers with identical settings and manage their settings using the profile created, while configuring the settings of the Security Server that does not belong to this group separately without creating a profile for it. A standalone Security Server that is not included in any profile is called an unassigned Security Server. You can configure an unassigned Security Server individually in the node of that Security Server.

Using profiles is optional. You can also configure the settings of Security Servers separately in the node of each Security Server.

If a company has multiple sites, allowance should be made for replication delays when creating and editing profiles, since the application stores profile information in Active Directory.

To use profiles, perform the following:

1. Create a profile (see section "Creating a profile" on page 59).
2. Configure the profile (see section "Configuring a Security Server in a profile" on page 59).
3. Add Security Servers to the profile (see section "Adding Security Servers to a profile" on page 60).
You may not be able to modify the Security Server settings if the Security Server has been added to a profile and profile settings have been inherited for it (see section "Configuring Security Servers in a profile" on page 59). The "lock" symbol appears next to the setting that cannot be edited. To specify Security Server settings that differ from the values of profile settings, remove the Security Server from the profile (see section "Removing a Security Server from a profile" on page 61).

You can create as many profiles as you wish, and add Security Servers to them or remove Security Servers from them at any time (see section "Removing a Security Server from a profile" on page 61). You may need to remove a Security Server from the profile, for example, in the following cases:

- If you need to specify Security Server settings that differ from those of a profile.
- If you need to add a Security Server to another profile (in this case, you should first remove it from the profile to which it has been added earlier).

If you do not need an existing profile anymore, you can remove that profile from the application configuration (see section "Removing a profile" on page 62).

CREATING A PROFILE

To create a new profile:

1. In the Administration Console tree, expand the Profiles node.
2. Add a new profile in one of the following ways:
   - By selecting the Add profile item in the Action menu.
   - By selecting the Add profile item in the context menu of the Profiles node.
   - By clicking the Add profile button in the workspace of Administration Console.
   - By clicking the Add profile link in the quick access bar.
3. In the Create profile window that opens, enter a profile name.
4. Click OK.

The child node with the name of the created profile appears within the Profiles node.

To be able to use the profile, you have to configure it (see section "Configuring Security Servers in a profile" on page 59) and add Security Servers to it (see section "Adding Security Servers to a profile" on page 60).

CONFIGURING SECURITY SERVERS IN A PROFILE

You can configure the following general settings for Security Servers belonging to the same profile (in the child nodes of the profile):

- Configure the anti-virus protection settings (see section "Configuring anti-virus processing of objects" on page 74) and spam protection settings (see section "Configuring spam scanning" on page 84), and also additional Anti-Virus settings (see section "Configuring anti-virus scanning exclusions" on page 75) in the Server protection node;
- Configure the schedule of automatic database updates (see section "Configuring scheduled database updates" on page 65) and the update source (see section "Selecting an update source" on page 66) in the Updates node;
- Configure notification settings (see section "Configuring notifications" on page 102) in the Notifications and Settings nodes;
- Define the event log settings (see the section "Configuring logs" on page 111) and the diagnostics level (see the section "Configuring diagnostics level" on page 112) in the Settings node;
- Manage keys and configure settings of license expiry notification (see section "Configuring the license expiry notification" on page 45) in the Licensing node;
- Configure the report settings (see section "Reports" on page 104) in the Reports node.
These changes do not affect the following custom settings of Security Servers and actions taken by the application on Security Servers:

- Start of a background scan (see section "Configuring background scanning" on page 78) in the Server protection node.
- Start of a database update (see section "Starting a database update manually" on page 64) in the Updates node.
- Update center settings (see section "Designating a server as an update center and configuring its settings" on page 67) in the Updates node.
- Test notification (see section "Configuring notification delivery" on page 103) in the Notifications and Settings nodes.
- Backup settings (see section "Backup settings" on page 97) in the Settings node.

You will still be able to edit settings and perform operations only separately for each of the Security Servers (in the child nodes of each Security Server or in the profile node in the tree of the Servers node for each Security Server).

**SPECIFICS OF MANAGING PROFILES IN A MICROSOFT EXCHANGE DATABASE AVAILABILITY GROUP**

If you make changes in the Exchange Administration Console to the configuration of a DAG that has been added to a profile in Kaspersky Security, consider the following specifics of the settings of Security Servers belonging to this DAG in Kaspersky Security:

- If you install Kaspersky Security on a Microsoft Exchange server belonging to a DAG that has been added to a profile, the settings of this profile are applied to the relevant Security Server in Kaspersky Security after installation.

- If you use the Exchange Administration Console to add a Microsoft Exchange server with Kaspersky Security installed to a DAG that has been added to a profile in Kaspersky Security, the settings of this profile are applied to the relevant Security Server in Kaspersky Security. If the DAG has not been added to a profile, individual settings of this DAG are applied to the relevant Security Server in Kaspersky Security.

- If you use the Exchange Administration Console to combine several Microsoft Exchange servers with the application installed into a new DAG, the settings of this DAG are applied to the relevant Security Servers in Kaspersky Security. In other words, the common default settings are applied (except for the list of protected storages and public folders), while the individual settings of servers and the settings of the list of protected storages and public folders remain just like they were before the servers were added to the DAG.

  If servers had been added to profiles prior to being combined into a DAG, once combined they still appear not only in the list of DAG servers, but also in such profiles. However, you will not be able to manage the settings of such servers from the profiles. You can manage the settings of these servers only from the profile to which the DAG has been added, or the individual settings of the DAG (if the DAG has not been added to a profile). If necessary, you can remove servers shown in profiles manually.

- If you use the Exchange Administration Console to remove a Microsoft Exchange server with the application installed from a DAG that has been added to a profile in Kaspersky Security, the corresponding Security Server is removed from the profile in Kaspersky Security and gets the default settings. After being removed from the DAG, this Security Server is no more displayed in the list of profile servers. You have to add it manually to the list of protected Microsoft Exchange servers (see the section "Adding Security Servers to Administration Console" on page 47) or to one of the profiles (see the section "Adding Security Servers to a profile" on page 60) and configure it (see the section "Configuring Security Servers in a profile" on page 59).

**ADDING SECURITY SERVERS TO A PROFILE**

To add Security Servers to a profile:

1. In the Administration Console tree, expand the Profiles node.
2. Select the node of the profile to which you want to add a Security Server, or expand the node of the profile and select the Servers node.
3. One the wizard for adding the Security Server to the profile in one of the following ways:
   - By selecting the **Add server** item in the **Action** menu.
   - By selecting the **Add server** item in the context menu of the node.
   - By clicking the **Add server** link in the quick access bar.
   - By clicking the **Add server** button in the workspace of Administration Console (only when a profile node is selected).

4. In the **Server selection** window of the Wizard, in the **Unassigned servers** field select Security Servers that you want to add to the profile.
   The **Unassigned servers** field displays Security Servers that have been added to none of the profiles.

5. In the **Server selection** window of the Wizard, click the **>>** button.
   The selected Security Servers appear in the **Added to profile** field.

6. Click the **Next** button.

7. In the **Confirmation** window of the Wizard that opens, click the **Finish** button.
   The Security Servers that have been added appear on the list of servers in the workspace of the profile node and in the profile node in the **Servers** node tree. Within 5 minutes, the application will apply the general settings of Security Servers of the profile (see section "Configuring Security Servers in a profile" on page 59) to the Security Servers that have been added to the profile.

---

You can add DAG servers to a profile only all at once. When a DAG is added to a profile, all servers and all their roles (including the Hub Transport role) are added to this profile.

A Security Server deployed on a computer on which a Microsoft Exchange server is deployed in the Edge Transport role cannot be added to the profile.

After a Security Server has been added to a profile, the license is applied to it at the profile level even if this Security Server had a different active license before it was added to this profile.

---

**REMOVING A SECURITY SERVER FROM A PROFILE**

To remove a Security Server from a profile:

1. In the Administration Console tree, expand the **Profiles** node.

2. Select the Security Server you want to remove in one of the following ways:
   - Select the node of the profile from which you want to remove the Security Server and, in the server list appearing in the workspace, select the Security Server that you want to remove.
   - Expand the node of the profile from which you want to remove the Security Server, expand the **Servers**, and select the Security Server that you want to remove in the server list.

3. Remove the selected Security Server in one of the following ways:
   - If you have selected a Security Server in the workspace, click the **Remove server** button.
   - If you have selected a Security Server in the server list of the **Servers** node, remove the Security Server in one of the following ways:
     - Select the **Remove** item in the **Action** menu.
     - Select the **Remove** item in the context menu of the node
     - Click the **Remove** link in the quick access bar.

4. In the window that opens, confirm server removal.
   Within 5 minutes, the application will remove the Security Server from the list of servers in the workspace of the profile node and from the **Servers** node in the tree of the profile node. These changes will not impact the settings of the Security Server, but you will no longer be able to adjust them from the profile; you will be able to adjust them individually for the Security Server in the node of this Security Server.
You can remove DAG servers from a profile only all at once.

After a Security Server has been removed from a profile, it continues to be subject to the license at the level of the profile from which it has been removed.

**REMOVING A PROFILE**

To remove a profile:

1. In the tree of the Administration Console, select the profile you want to remove in one of the following ways:
   - Select the **Profiles** node and select the profile that you want to remove in the profile list appearing in the workspace.
   - Expand the **Profiles** node, and select the node of the profile that you want to remove in the list of nodes.

2. Remove the selected profile in one of the following ways:
   - If you have selected a profile in the workspace, click the **Remove profile** button.
   - If you have selected a node of a profile nested in the **Profiles** node, remove the profile in one of the following ways:
     - Select the **Remove** item in the **Action** menu.
     - Select the **Remove** item in the context menu of the profile node.
     - Click the **Remove** link in the quick access bar.

3. In the window that opens, confirm profile removal.

The application will remove the profile from the tree of the **Profiles** node. Security Servers included in the profile become unassigned. These modifications will not impact the settings of unassigned Security Servers, but you will be able to adjust all of the settings for each of the Security Servers only individually in the node of each server.
UPDATING PROGRAM DATABASES

This section explains how to update application databases and configure database updates.

In this section:

About program database updates ................................................................................................................................. 63
About update centers .................................................................................................................................................. 63
About database updates in configurations with a DAG of servers ............................................................................. 64
Updating databases manually ......................................................................................................................................... 64
Configuring scheduled databases updates .................................................................................................................. 65
Select update source ..................................................................................................................................................... 66
Configuring the connection to the update source ....................................................................................................... 67
Configuring the proxy server settings ........................................................................................................................ 67
Designating a server as an update center and configuring its settings ........................................................................ 67

ABOUT PROGRAM DATABASE UPDATES

Updates of Kaspersky Security application databases keeps Microsoft Exchange server protection up to date.

New viruses and other threats as well as new kinds of spam appear on a daily basis worldwide. Information about threats and spam and ways to neutralize them is contained in the application databases, i.e., those of Anti-Virus, DLP Module, and Anti-Spam. Application databases have to be updated regularly to enable timely detection of new threats and spam messages.

You are advised to update the application databases immediately after installation, as the databases included in the distribution kit may be out of date by the time you install your application. The databases of Anti-Virus and DLP Module on Kaspersky Lab servers are updated every hour. The Anti-Spam database is updated every five minutes. We recommend configuring scheduled database updates to be performed at the same intervals (see section "Configuring scheduled databases updates" on page 65).

Kaspersky Security can retrieve database updates from the following update sources:

- From Kaspersky Lab's update servers on the Internet
- From another HTTP server or FTP server, such as your Intranet server
- From a local update source, such as a local or network folder
- From the update center – one of the servers with Kaspersky Security installed, which has been designated as the update center (see section "About update centers" on page 63).

Database updates can be performed manually or according to schedule.

The application's functionality may change after an update of the application databases.

ABOUT UPDATE CENTERS

Any Microsoft Exchange server with Kaspersky Security installed can be designated as an update center (see section "Designating a server as an update center and configuring its settings" on page 67). Update centers receive updated databases from Kaspersky Lab servers and can serve as sources of updates for application databases (see section "Selecting the update source" on page 66) of other Microsoft Exchange servers with the application installed.
Update centers can be useful in the following cases:

- If your company has several Microsoft Exchange servers with the application installed, you can designate one of the Microsoft Exchange servers as an update center that receives databases from Kaspersky Lab servers and set it as an update source for other Microsoft Exchange servers of the company. This reduces the amount of Internet traffic, maintains databases on all Microsoft Exchange servers in an identical state, and eliminates the need to configure the Internet connection for each Microsoft Exchange server and monitor the security of such connections.

- If the corporate network has geographically distributed server segments with slow data links, you can create a dedicated update center for each regional segment to receive database updates from Kaspersky Lab servers. This reduces the amount of network traffic between regional segments and speeds up the distribution of updates to all servers on the corporate network.

**ABOUT DATABASE UPDATES IN CONFIGURATIONS WITH A DAG OF SERVERS**

In configurations with a DAG of Microsoft Exchange servers, database update settings are the same for the entire DAG of servers. This enables centralized updates of databases on all servers that are part of the configuration.

You can configure centralized database updates in the following ways:

- **From Kaspersky Lab’s update servers.** When this method is used, each server in the DAG connects to Kaspersky Lab update servers at the specified time independently of other servers, which causes a great amount of Internet traffic. This method is therefore not recommended for configurations with a large number of servers. Another downside of this method is the need to configure the Internet connection on each server in the configuration. The advantage of this method is high reliability, as updates are performed directly from Kaspersky Lab servers without intermediaries.

- **From an intermediate server or network folder.** When this method is used, servers belonging to a DAG download updates from an intermediate HTTP server or FTP server or network folder located outside of the configuration of Microsoft Exchange servers. This method reduces the amount of Internet traffic while ensuring fast and synchronized updates on all servers in the configuration, but also entails extra expenses on the upkeep of intermediate hardware.

- **From an update center.** This method involves designating one of the servers in the DAG as an update center (see section "Designating a server as an update center and configuring its settings" on page 67). The advantages of this method are low Internet traffic, fast and synchronized updates on all servers in the configuration. When this method is used, however, higher reliability requirements apply to the server designated as the update center.

**UPDATING DATABASES MANUALLY**

To view information about Anti-Virus and DLP Module database updates and update them if necessary:

1. In the Administration Console tree, expand the node of a Security Server.
2. Select the Updates node.
3. In the workspace, in the Anti-Virus and DLP Module database update section, the following information is displayed:
   - **Result of the last update.** Information about the Anti-Virus and DLP Module database update status.
   - **Release date of the databases.** Time when the Anti-Virus and DLP Module databases currently used in the application were published on the Kaspersky Lab server (UTC).
   - **Records.** Number of virus signatures in the current version of the Anti-Virus and DLP Module databases.
4. To update Anti-Virus and DLP Module databases, click the Start update button.
5. To stop the update procedure, click the Stop button.

If the application is running in a DAG of Microsoft Exchange servers, you should update the databases of Anti-Virus and DLP Module on each of the servers included in the DAG.
To view information about Anti-Spam database updates and update them if necessary:

1. In the Administration Console tree, expand the node of a Security Server.
2. Select the Updates node.
3. In the workspace, in the Anti-Spam databases update section, the following information is displayed:
   - Result of the last update. Information about the Anti-Spam database update status.
   - Release date of the databases. Time when the Anti-Spam database currently used in the application became available on the server of Kaspersky Lab (UTC).
4. To update Anti-Spam databases, click the Start update button.
5. To stop the update procedure, click the Stop button.

CONFIGURING SCHEDULED DATABASES UPDATES

To configure scheduled Anti-Virus and DLP Module database updates:

1. Perform the following steps in the Administration Console tree:
   - To configure scheduled Anti-Virus and DLP Module database updates for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To configure scheduled Anti-Virus and DLP Module database updates for Security Servers belonging to one profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to configure Anti-Virus and DLP Module database updates.
2. Select the Updates node.
3. Open the Anti-Virus and DLP Module database update section in the workspace.
4. Select one of the following options from the Run mode drop-down list:
   - Periodically. In the every N minutes / hours / days spin box, specify the frequency of database updates in minutes / hours / days.
   - Daily. In the spin box on the right, specify the exact local time of the server.
   - On selected day. Select the check boxes next to the days of the week when you would like to update the Anti-Virus database, and specify the update time.
5. Click the Save button.

If the application is running in a configuration with a DAG of Microsoft Exchange servers, the scheduled automatic Anti-Virus and DLP Module database update settings, configured on one of the servers will be automatically applied to all servers within the DAG. It is not required to configure scheduled updates on the remaining servers within this DAG.

To configure scheduled Anti-Spam database updates:

1. Perform the following steps in the Administration Console tree:
   - To configure scheduled Anti-Spam database updates for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To configure scheduled Anti-Spam database updates for Security Servers belonging to one profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to configure Anti-Spam database updates.
2. Select the Updates node.
3. Open the Anti-Spam databases update section in the workspace.
4. Select one of the following options from the Run mode drop-down list:
   - Periodically. In the every N minutes / hours / days spin box, specify the frequency of database updates in minutes / hours / days.
   - Daily. In the spin box on the right, specify the exact local time of the server.
   - On selected day. Select the check boxes next to the days of the week when you would like to update the Anti-Spam database, and specify the update time.
5. Click the Save button.
SELECTING AN UPDATE SOURCE

To choose an Anti-Virus database update source:

1. Perform the following steps in the Administration Console tree:
   - To choose an Anti-Virus database update source for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To choose an Anti-Virus database update source for Security Servers belonging to one profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to choose an update source.

2. Select the Updates node.

3. Expand the Anti-Virus database update section in the workspace and select one of the following options:
   - To download updates from Kaspersky Lab servers, select the Kaspersky Lab’s update servers item. This source of updates is set by default.
   - To download updates from an intermediate server, local or network folder, select the HTTP server, FTP server, local or network folder item. Then specify the server address or the full path to a local or network folder in the entry field.
   - To download updates from an update center, select the Update center storage item. Then select the server that is the update center in the drop-down list.

You can select this update source if at least one update center has been created in your configuration (see section "Designating a server as an update center and configuring its settings" on page 67). If the Microsoft Exchange server for which you are selecting an update source is deployed in an Edge Transport role, the name of the server designated as the update server may be missing from the drop-down list. In this case, manually type the name of the server that is the designated update center.

4. Click the Save button.

If the application is running in a configuration with a DAG of Microsoft Exchange servers, the automatic Anti-Virus database update settings (in particular, the source of updates) configured on one of the servers will be automatically applied to all servers within the DAG. It is not necessary to configure update settings on other servers.

To choose an Anti-Spam database update source:

1. Perform the following steps in the Administration Console tree:
   - To choose an Anti-Spam database update source for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To choose an Anti-Spam database update source for Security Servers belonging to a profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to choose an update source.

2. Select the Updates node.

3. Expand the Anti-Spam databases update section in the workspace and perform one of the following actions:
   - To download updates from Kaspersky Lab servers, select the Kaspersky Lab’s update servers item. This source of updates is set by default.
   - To download updates from an intermediate server, local or network folder, select the HTTP server, FTP server, local or network folder item. Then specify the server address or the full path to a local or network folder in the entry field.
   - To download updates from an update center, select the Update center storage item. Then select the server that is the update center in the drop-down list.

You can specify this update source if at least one update center has been created in your configuration. If the Microsoft Exchange server for which you are selecting an update source is deployed in an Edge Transport role, the name of the server designated as the update server may be missing from the drop-down list. In this case, manually type the name of the server that is the designated update center.

4. Click the Save button.
CONFIGURING THE CONNECTION TO THE UPDATE SOURCE

To configure the connection to an update source:

1. Perform the following steps in the Administration Console tree:
   - To configure the connection to an update source for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To configure the connection to an update source for Security Servers belonging to a profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to configure the connection to an update source.

2. Select the Updates node.

3. In the workspace, open the Connection settings section.

4. If your Internet connection is established through a proxy server, enable the option to Use proxy server.

5. In the Maximum connection timeout spin box, enter the maximum time (in seconds) that the server will wait for a connection to the update source.

   The Microsoft Exchange server will be attempting to connect to the update source during this time. The default value of this setting is 60 seconds. You may need to increase it if you have a slow Internet connection, for example.

6. Click the Save button.

   If the Internet connection is established using a proxy server, you have to configure the proxy server settings (see section “Configuring the proxy server settings” on page 67).

CONFIGURING PROXY SERVER SETTINGS

To configure the proxy server settings, perform the following steps:

1. Perform the following steps in the Administration Console tree:
   - To configure the connection to a proxy server for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To configure the connection to a proxy server for Security Servers belonging to a profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to configure the connection to a proxy server.

2. Select the Settings node.

3. In the workspace, expand the Proxy server settings section.

4. Enter the proxy server address in the Proxy server address field.

5. Specify the proxy server port number in the Port field.

   The default port number is 8080.

6. If authentication is required to connect to the specified proxy server, select the Use authentication check box and enter the account name in the Account field and password in the Password field.

7. Click the Save button.

DESIGNATING A SERVER AS AN UPDATE CENTER AND CONFIGURING ITS SETTINGS

We strongly advise against designating an update center and configuring its settings when migrating to a new version of the application on servers operating as part of a configuration with a DAG of Microsoft Exchange servers. The operations described in this section should be performed only after completing the migration of all servers to the new version of the application (see page 30).
We strongly advise against designating a virtual Microsoft Exchange server as an update center.

A Microsoft Exchange server that is an update center must have a constant Internet connection and 500 MB of extra disk space.

To designate a server as an update center and configure its settings:

1. In the Administration Console tree, expand the node of a Security Server.
2. Select the Updates node.
3. In the workspace, expand the Update center settings section.
4. Select the Server functions as Update Center check box.
5. Select the update source from which the update center will be receiving databases.
   - To download updates to the update center from Kaspersky Lab servers, select the Kaspersky Lab's update servers item. This source of updates is set by default.
   - To download updates to the update center from an intermediate server, local or network folder, select the HTTP server, FTP server, local or network folder item. Then specify the server address or the full path to a local or network folder in the entry field.
   - To download updates to the update center from another update center, select the Update center storage item. Then select the server that is the update center in the drop-down list.
6. Configure the database update schedule for the update center. To do so, select one of the following options from the Run mode drop-down list:
   - Periodically. In the every N minutes / hours / days spin box, specify the frequency of database updates.
   - Daily. Define the precise local time of the server in HH:MM format.
   - On selected day. Select the check boxes next to the days of the week when you would like to update the database, and specify the update time.

We strongly advise against selecting the Manual database update start mode for the update center, as this mode makes it impossible to ensure that databases stay up to date on the update center and on all servers that use it as an update source.

7. If the Internet connection is established via a proxy server, select the Use proxy server for the Update Center check box and configure the proxy server settings by selecting one of the following options:
   - If you want to connect the update center to the Internet using the proxy server settings specified in the Settings node, choose the option Use proxy server settings specified in the Settings section.
   - If you want to connect the update center to the Internet using other proxy server settings, select the option Specify proxy server settings for update downloads by the Update Center and perform the following:
     a. Type the proxy server address and port in the Proxy server address and Port fields, respectively.
     b. If authentication is required to connect to the specified proxy server, select the Use authentication check box and enter the account name in the Account field and password in the Password field.
8. Click the Save button.

The selected Microsoft Exchange server is designated as an update center. You can later select it as an update source for other servers (see section "Selecting the update source" on page 68).
ANTI-VIRUS PROTECTION

This section contains information about Anti-Virus protection of a Microsoft Exchange server, background scanning of storages, and ways to configure protect and scan settings.

IN THIS SECTION:

- About Anti-Virus protection ................................................................. 69
- About background scanning ................................................................. 70
- About participation in Kaspersky Security Network ................................ 72
- Enabling and disabling anti-virus server protection .............................. 72
- Enabling and disabling KSN in Anti-Virus ........................................... 73
- Configuring object processing settings .................................................. 74
- Configuring mailbox and public folder protection settings .................... 74
- Configuring anti-virus scan exclusions ................................................ 75
- Configuring background scan settings .................................................. 78

ABOUT ANTI-VIRUS PROTECTION

One of the main purposes of Kaspersky Security is the anti-virus protection, which aims the application at scanning the mail flow and messages in mailboxes for viruses and other security threats, as well as disinfecting infected messages and other Microsoft Exchange objects, such as messages, tasks, or entries in shared folders.

Hereinafter, any information and instructions on how to perform actions on messages without affecting the integrity are also applicable to other Microsoft Exchange objects (such as tasks, appointments, meetings, entries), if there is no other specifically assigned condition.

General performance principles of Anti-Virus

Anti-Virus scans messages using the latest downloaded version of databases, Heuristic Analyzer, and the Kaspersky Security Network cloud service if this service is enabled in Anti-Virus settings (see section "Enabling and disabling KSN in Anti-Virus" on page 73).

Anti-Virus scans the message body and attachments in any format.

Kaspersky Security differentiates between the following types of objects that are scanned: a simple object (message body or a simple attachment, such as an executable file) and a container object, which consists of several objects (such as an archive or a message with another message attached).

When scanning multivolume archives, the application processes each volume as a separate object. In this case, Kaspersky Security can detect malicious code only if the code is fully located in one of the volumes. If the malicious code is also divided into parts during a partial download, it will not be detected during the scan. In this situation, the malicious code may propagate after the object is restored as one entity. Multiple-volume archives can be scanned after they are saved to the hard drive by the anti-virus application installed on the user’s computer.

If necessary, you can define a list of objects that should not be scanned for viruses. Archives, all container objects with a nesting level above the specified value, files matching name masks, and messages addressed to specific recipients can be excluded from scanning (see section "Configuring anti-virus scan exclusions" on page 75).

Files over 1 MB will be saved to the Store working folder for processing. The Store folder is located in the Data folder of the application. The Data folder also contains the temporary files storage – the Tmp folder. The Store and Tmp folders should be excluded from scanning by anti-virus applications running on computers with a Microsoft Exchange server installed.
Following the scan, Anti-Virus assigns one of the following statuses to each message:

- **Infected**: the object has been scanned and contains at least one known virus.
- **Not infected**: the object has been scanned and contains no viruses.
- **Protected**: the object has not been scanned, protected with a password.
- **Corrupted**: the object has not been scanned and is corrupted.

If an e-mail message or a part of it is infected, Anti-Virus processes the detected malicious object in accordance with the specified settings.

In the settings of Anti-Virus, you can configure the actions that the application will perform on messages containing malicious objects. You can configure the following actions:

- **Allow**: Anti-Virus skips the message and the malicious object which it contains.
- **Delete the object**: Anti-Virus deletes the malicious object but allows the message to pass.
- **Delete the message**: Anti-Virus deletes the message along with the malicious object.

When a malicious object gets deleted on a Microsoft Exchange server deployed as a Mailbox, the message or attachment containing the malicious object is replaced with a text file containing the name of the malicious object, the release date of the database used to detect the malicious object, and the name of the Microsoft Exchange server where the object was detected. When a malicious object is detected on a Microsoft Exchange server deployed in a Hub Transport role or Edge Transport role, the application also adds the **Malicious object deleted** prefix to the message subject.

Before being processed by Anti-Virus, a copy of the item can be saved in Backup (see the section "About Backup" on page 93).

Anti-Virus consists of two application modules: **Anti-Virus for the Hub Transport role** and **Anti-Virus for the Mailbox role**.

**Anti-Virus for the Hub Transport role**

Anti-Virus for the Hub Transport role scans in real time all e-mail messages arriving at the Microsoft Exchange server. It processes both incoming and outgoing e-mail traffic as well as the stream of transit messages. If anti-virus protection of the server is enabled, traffic scanning starts and stops simultaneously with the starting and stopping of the Microsoft Exchange server.

**Anti-Virus for the Mailbox role**

Anti-Virus for the Mailbox role scans messages and other Microsoft Exchange items located in users' mailboxes within an organization and shared folders, searching for viruses and other security threats.

Protection provided by Anti-Virus for the Mailbox role covers all mailboxes and shared folders that are located in protected mailbox storage areas and protected storage areas for shared folders, respectively. You can include and exclude from Anti-Virus protection mailbox storage areas and storage areas for shared folders individually (see the section "Configuring the protection of mailboxes and shared folders" on page 74).

Microsoft Exchange 2013 servers feature no storage areas for shared folders. Microsoft Exchange 2013 servers store mailboxes and shared folders in common storage areas.

When a user whose mailboxes are protected creates messages in public folders of unprotected Microsoft Exchange servers, Kaspersky Security does not scan such messages. If messages are transferred from public folders of an unprotected storage to a protected one, the application scans them. During data replication between protected and unprotected storages, any changes made by the application as a result of the anti-virus scan are not synchronized.

**ABOUT BACKGROUND SCANNING**

**Background scanning** is an operation mode of Anti-Virus for the Mailbox role when it scans messages and other Microsoft Exchange objects stored on a Microsoft Exchange server, searching for viruses and other security threats with the latest version of the anti-virus databases. Using background scan mode decreases the load on the servers during busy hours and increases the security level of the e-mail infrastructure in general.

During a background scan, Kaspersky Security, in accordance with the current settings, receives email messages and other Microsoft Exchange objects stored in protected storage areas for mailboxes and shared folders on a Microsoft Exchange server (see the section "Configuring the protection of mailboxes and shared folders" on page 74), such as tasks, appointments, meetings, entries, etc.
Hereinafter, any information and instructions on how to perform actions on messages are also applicable to other Microsoft Exchange objects (such as tasks, appointments, meetings, entries), if there is no other specifically assigned condition.

If a message has not been scanned against databases of the latest version, the application forwards it to the Anti-Virus module for the Mailbox role for processing. If any infected objects are detected during this background scan, Anti-Virus processes them in accordance with the settings defined for the Mailbox role (see the section “Configuring the anti-virus processing of objects” on page 74), using the following algorithm:

If an infected object is detected in a message or another Microsoft Exchange object, and the Delete object or Delete message action is selected in the settings of Anti-Virus, the latter attempts to disinfect that object.

If disinfection has been successful, Anti-Virus replaces the infected object with the disinfected one.

If disinfection has failed, Anti-Virus performs the actions specified in the table.

Table 8. Actions performed by Anti-Virus if disinfection of an infected object fails

<table>
<thead>
<tr>
<th>WHERE WAS THE INFECTED OBJECT FOUND?</th>
<th>ACTION SELECTED</th>
<th>ACTION OF ANTI-VIRUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>In a message</td>
<td>Delete message</td>
<td>Anti-Virus deletes the message along with the infected object.</td>
</tr>
<tr>
<td></td>
<td>Delete object</td>
<td>Anti-Virus replaces the infected object (attachment) with a text file informing that the infected object was deleted.</td>
</tr>
<tr>
<td>In another Microsoft Exchange object (such as a task, meeting, or entry)</td>
<td>Delete message</td>
<td>Anti-Virus replaces the infected object (attachment) with a text file informing that the infected object was deleted.</td>
</tr>
<tr>
<td></td>
<td>Delete object</td>
<td>Anti-Virus replaces the infected object (attachment) with a text file informing that the infected object was deleted.</td>
</tr>
</tbody>
</table>

Anti-Virus does not delete Microsoft Exchange objects completely if they are not messages. Only infected attachments can be deleted from them.

If the Save copy of object in Backup check box is selected in the settings of Anti-Virus for Mailboxes, Kaspersky Security moves a copy of the object to Backup before processing that object. If the object (e.g., a task) features no From or To field, the missing field will be replaced in Backup with the address of the user whose mailbox stores the object.

Background scanning of messages can be repeated. Anti-Virus performs repeated background scanning of messages that have been scanned earlier after you update the anti-virus databases. A background scan can be run manually or upon a schedule (see the section “Configuring background scanning” on page 78).

Background scanning may lead to a slowdown in the Microsoft Exchange server's operation. You are therefore recommended to use the background scanning when the workload on mail servers is at its minimum, e.g., by night.

Depending on the version of the protected Microsoft Exchange server, Kaspersky Security uses the following technologies for background scanning:


The background scanning feature on a Microsoft Exchange 2013 server has the following specifics:

- To perform background scans, the application uses an EWS server based locally on the protected Microsoft Exchange 2013 server. When running a background scan on the Microsoft Exchange 2013 servers included in the profile, it runs concurrently, using the local EWS servers, which are available on each of the protected servers. If the local EWS server is not available, the application records a message with detailed information about the error to the event log of the protected server.

- When handling a Microsoft Exchange 2013 server, a background scan can only be performed if the application service account has been assigned the ApplicationImpersonation role from the set of built-in roles named Role Based Access Control (RBAC) of Microsoft Exchange 2013. Otherwise, when attempting to run a background scan, Kaspersky Security records an error message to Microsoft Windows Event Log. The Application Setup Wizard assigns this role to the application service account automatically when installing or upgrading the application. If this assignment has not been completed by the Application Setup Wizard due to an error, it must be performed manually with Microsoft Exchange administration tools.
Due to hardware restrictions applied to Microsoft Exchange 2013 servers, Anti-Virus only scans shared folders that meet the following condition: at least one user exists who has the following set of rights of access to that shared folder:

- Folder visible
- Read items
- Edit all
- Delete all.

**ABOUT PARTICIPATION IN KASPERSKY SECURITY NETWORK**

To protect your computer more effectively, Kaspersky Security uses data that is collected from users around the globe. Kaspersky Security Network is designed to collect such data.

Kaspersky Security Network (KSN) is an infrastructure of online services providing access to Kaspersky Lab's online knowledge base with information about the reputation of files, online resources, and software. The use of data from Kaspersky Security Network ensures faster response by Kaspersky Security to unknown threats, improves the effectiveness of some protection components, and reduces the risk of false positives.

Thanks to your participation in Kaspersky Security Network, Kaspersky Lab is able to promptly gather information about types and sources of new threats, develop solutions for neutralizing them, and process spam messages with a high level of accuracy.

When you participate in Kaspersky Security Network, certain statistics are collected while Kaspersky Endpoint Security is running and are automatically sent to Kaspersky Lab (see section "About data submission" on page 40). Also, additional checking at Kaspersky Lab may require sending files (or parts of files) that are imposed to an increased risk of being exploited by intruders to do harm to the user's computer or data.

You can enable or disable Kaspersky Security Network separately for Anti-Virus (see section "Enabling and disabling KSN in Anti-Virus" on page 79) and Anti-Spam (see section "Configuring spam and phishing scan settings" on page 84).

Participation in Kaspersky Security Network is voluntary. You can opt out of participating in Kaspersky Security Network at any time. No personal data of the user is collected, processed, or stored. The types of data that Kaspersky Security sends to Kaspersky Security Network are described in the KSN Statement.

**ENABLING AND DISABLING ANTI-VIRUS SERVER PROTECTION**

If the anti-virus server protection is enabled, anti-virus scanning of e-mail traffic is started or stopped together with the Microsoft Exchange server. Background scanning of storages (see section "Configuring background scanning" on page 78) can be launched manually or automatically according to schedule.

Disabling anti-virus protection of the server considerably increases the risk of malware infiltrating the e-mail system. You are advised not to disable anti-virus protection unless absolutely necessary.

Anti-virus protection of a Microsoft Exchange server deployed in Mailbox and Hub Transport roles is enabled separately.

To enable or disable Anti-Virus protection of the Microsoft Exchange server in the Mailbox role:

1. Perform the following steps in the Administration Console tree:
   - To enable or disable anti-virus protection of an unassigned Security Server, maximize the node of the relevant Security Server;
   - To enable or disable anti-virus protection of Security Servers belonging to a profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to configure anti-virus protection.

2. Select the Server protection node.
3. In the workspace, on the Protection for Mailbox role tab, in the Anti-Virus scan settings section, perform one of the following actions:
   - Select the Enable Anti-Virus protection for the Mailbox role check box if you want to enable Anti-Virus protection of the Microsoft Exchange server.
   - Clear the Enable Anti-Virus protection for the Mailbox role check box if you want to disable Anti-Virus protection of the Microsoft Exchange server.
4. Click the Save button.

If the application is running on a DAG of Microsoft Exchange servers, anti-virus server protection enabled for the Mailbox role on one of the servers is enabled automatically on the remaining servers within this DAG. Enabling anti-virus protection for the Mailbox role on the remaining DAG servers is not necessary.

To enable Anti-Virus protection of the Microsoft Exchange server in the Hub Transport role:
1. Perform the following steps in the Administration Console tree:
   - To enable or disable anti-virus protection of an unassigned Security Server, maximize the node of the relevant Security Server;
   - To enable or disable anti-virus protection of Security Servers belonging to a profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to configure anti-virus protection.
2. Select the Server protection node.
3. In the workspace, on the Protection for Hub Transport role tab, in the Anti-Virus scan settings section, perform one of the following actions:
   - Select the Enable Anti-Virus protection for the Hub Transport role check box if you want to enable Anti-Virus protection of the Microsoft Exchange server.
   - Clear the Enable Anti-Virus protection for the Hub Transport role check box if you want to disable Anti-Virus protection of the Microsoft Exchange server.
4. Click the Save button.

**ENABLING AND DISABLING KSN IN ANTI-VIRUS**

To enable or disable KSN in Anti-Virus:
1. Perform the following steps in the Administration Console tree:
   - To enable or disable KSN in Anti-Virus for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To enable or disable KSN in Anti-Virus for Security Servers belonging to a profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to enable or disable it.
2. Select the Server protection node.
3. In the workspace, select the Advanced Anti-Virus settings tab.
4. Select the Use Kaspersky Security Network (KSN) check box.
   
   The Use Kaspersky Security Network (KSN) check box is available when the I accept the KSN Statement check box is selected in the KSN settings section of the Settings node.
5. If necessary, specify the timeout for requests to a KSN server in the Maximum timeout for a KSN request scroll field.
   
   The default value is 5 sec.
6. Click the Save button.
CONFIGURING ANTI-VIRUS PROCESSING OF OBJECTS

You can configure Anti-Virus processing of objects by selecting an action to be taken by the application on each type of objects.

The settings of anti-virus processing of Anti-Virus objects for the Mailbox role and the settings of Anti-Virus for the Hub Transport role must be defined independently.

To configure object processing settings:

1. Perform the following steps in the Administration Console tree:
   - To configure the settings of anti-virus processing of objects for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To configure the settings of anti-virus processing of objects for Security Servers belonging to a profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to configure the settings of anti-virus processing of objects.
2. Select the Server protection node.
3. Perform one of the following steps:
   - To define the object processing settings for a Microsoft Exchange server in the Mailbox role, on the Protection for the Mailbox role tab in the workspace, expand the Anti-Virus scan settings section.
   - To define the object processing settings for the Hub Transport role, on the Protection for Hub Transport role tab in the workspace, expand the Anti-Virus scan settings section.
4. In the Objects processing settings section, use the Infected object drop-down list to select the action to be taken on infected objects:
   - Select Allow to have the application allow the message and the infected object contained in it.
   - Select Delete object to have the application delete the infected object but allow the message.
   - Select Delete message to have application delete the message containing the infected object with all attachments.
5. Password protection may prevent anti-virus scanning of protected objects. In the Protected object drop-down list, select an action to be taken on protected objects:
   - Select Allow to have the application allow messages with password-protected objects.
   - Select Delete message to have the application delete messages with password-protected objects.
6. In the Corrupted object drop-down list, select an action:
   - Select Allow to have the application allow messages with corrupted objects.
   - Select Delete message to have the application delete messages with corrupted objects.
7. To save a copy of an object in Backup before processing it (see the section "About Backup" on page 93), select the Save a copy of the object in Backup check box.

If the application is running on a DAG of Microsoft Exchange servers, object processing settings configured for a server deployed in the Mailbox role on one of the servers are automatically applied to other servers within this DAG. Configuring the object processing settings for the Mailbox role on other servers of the DAG is not necessary. However, the object processing settings for the Hub Transport role have to be configured individually on each of the DAG servers.

CONFIGURING MAILBOX AND PUBLIC FOLDER PROTECTION SETTINGS

The application can protect the number of mailboxes that does not exceed the limitation of the active key (see section "Viewing information about installed keys" on page 43). If this number is insufficient, you can alternate protection between mailboxes. To do so, you have to move to unprotected storage the mailboxes that need no protection. By default, the application also protects all public folders of the mail server. You can remove protection from public folders if you think that scanning them would be redundant.
By default, the application protects those storages of mailboxes and storages of public folders on the protected Microsoft Exchange server, which already existed at the time when the application was installed, as well as all newly-created storages.

**To configure the protection settings for mailboxes and public folders:**

1. Perform the following steps in the Administration Console tree:
   - To configure the protection settings for mailboxes and public folders for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To configure the protection settings for mailboxes and public folders for Security Servers belonging to a profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to configure the protection settings for mailboxes and public folders.

2. Select the Server protection node.

3. On the Anti-virus protection for Mailbox role tab in the workspace, expand the Protection for mailboxes section.

The lists of Protected mailbox storages and Protected public folder storages show the mailbox storages and public folders on the protected Microsoft Exchange server.

If the application is running in a DAG of Microsoft Exchange servers, these lists enumerate mailbox storages and public folder storages on all the servers within this DAG.

When viewed from a profile, the Protected mailbox storages list shows only the protected storages of those Microsoft Exchange servers on which Anti-Virus for the Mailbox role is deployed.

4. In the Protected mailbox storages list, select the check boxes of the mailbox storages for which protection should be enabled.

5. In the Protected public folder storages list, select the check boxes of the public folder storages for which protection should be enabled.

6. Click the Save button.

**CONFIGURING ANTI-VIRUS SCAN EXCLUSIONS**

To ease the load on the server during an anti-virus scan, you can configure scan exclusions by limiting the range of objects to scan. Anti-virus scan exclusions apply to both e-mail traffic scanning and background scanning of storages.

You can configure anti-virus scan exclusions as follows:

- Disable scanning of archives and containers (see section "Configuring scanning of attached containers and archives" on page 78).
- Configure exclusions by file name masks (see section "Configuring exclusions by file name masks" on page 77).
- Configure exclusions by recipient's address.

Messages addressed to the specified recipients are excluded from the anti-virus scan.

If the application is running on a DAG of Microsoft Exchange servers, the scanning exclusions configured on one of the servers are automatically applied to all Microsoft Exchange servers within the DAG. Configuring scanning exclusions on other servers within this DAG is not necessary.

**ABOUT TRUSTED RECIPIENTS**

You can exclude from scanning the messages addressed to specific recipients by specifying the addresses of these recipients in the list of trusted recipients (see the section "Configuring exclusions by recipient's address" on page 76). The list is empty by default.

You can add recipients' addresses to the list of trusted recipients in the form of entries of the following types:

- Active Directory objects:
  - User.
  - Contact.
• Distribution Group.
• Security Group.

It is recommended to add addresses in the form of entries of this type.

• SMTP addresses in the mailbox@domain.com format.

Entries of this type should be added when Anti-Virus is installed for the Hub Transport role or the address you want to exclude cannot be located in Active Directory.

To exclude a public folder from scanning by Anti-Virus for the Hub Transport role, you should add all of its SMTP addresses (if there are several of them) to the list of trusted recipients. If any of the SMTP addresses of the public folder are not on the list, messages arriving in the public folder can be scanned by Anti-Virus.

• Display Name.

Entries of this type should be added when Anti-Virus is installed for the Mailbox role or the address you want to exclude cannot be located in Active Directory.

• Public folders.

Entries of this type should be added if Anti-Virus has been installed for the Mailbox role. Public folders cannot be selected from Active Directory. The full path to the public folder should be specified when adding such entries.

When Anti-Virus is installed for the Mailbox role and the Hub Transport role and the address you want to exclude cannot be located in Active Directory, the list of trusted recipients should include two entries corresponding to this address: SMTP address and user / group name. Otherwise, messages sent to this address will not be excluded from the scan.

Recipients' addresses specified in the form of Active Directory objects are excluded from the anti-virus scan according to the following rules:

• If the recipient's address is specified as a User or a Contact, messages addressed to this recipient are excluded from scanning.

• If the address is specified as a Distribution Group, messages addressed to this distribution group are excluded from the scan. However, messages addressed personally to individual distribution group members are not excluded from the scan unless their addresses have been added to the list separately.

• If the address is specified as a Security Group, messages addressed to this group and its members are excluded from the scan. However, if a nested security group is a member of the specified Security Group, messages addressed to members of the nested security group are not excluded from the scan unless their addresses have been added to the list separately.

The application automatically updates user addresses received from Active Directory following changes to the relevant Active Directory accounts (for example, when a user's email address has changed or a new member has been added to a security group). This update is performed once a day.

**CONFIGURING EXCLUSIONS BY RECIPIENT’S ADDRESS**

You can exclude messages addressed to specific recipients by specifying the addresses of these recipients in the list of trusted recipients.

To configure exclusions by recipient’s address:

1. Perform the following steps in the Administration Console tree:
   - To configure exclusions by recipient addresses for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To configure exclusions by recipient addresses for Security Servers belonging to a profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to configure exclusions.

2. Select the Server protection node.

3. In the workspace, select the Advanced Anti-Virus settings tab.

4. Check the Do not scan messages for the following recipients box.
5. Add the recipient's address to the list of trusted addresses. To do so, perform the following:
   - To add an Active Directory account to the list:
     a. Click the button.
     b. In the window that opens, locate the relevant Active Directory account and click OK.
    Addresses selected in Active Directory are marked in the list by the following symbols:
    - users, contacts, distribution groups;
    - security groups.
   - To add an SMTP address, a user name, or a public folder to the list:
     - To add an SMTP address or a user name to the list, type it in the entry field and click the button.
     - To add a public folder, enter the path to the folder and click the button.
    Addresses added in this way are marked on the list by the icon.
    Addresses added in this way are not checked for their presence in Active Directory.

6. To remove a recipient's address from the list of trusted recipients, highlight the recipient's entry in the list and click the button.

7. To export a list of trusted addresses to file:
   a. Click the button.
   b. In the window that opens, specify the file name in the File name field.
   c. Click the Save button.

8. To import a list of trusted addresses from file:
   a. Click the button.
   b. In the window that opens, in the File name field specify the file containing the list of trusted addresses.
   c. Click the Open button.

9. Click the Save button.

**CONFIGURING EXCLUSIONS BY FILE NAME MASK**

To configure exclusions by file name masks:

1. Perform the following steps in the Administration Console tree:
   - To configure exclusions by file name masks for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To configure exclusions by file name masks for Security Servers belonging to a profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to configure exclusions.

2. Select the Server protection node.

3. In the workspace, select the Advanced Anti-Virus settings tab.

4. Check the Do not scan files matching the masks box.

5. Add a file name mask (hereinafter also "mask") to the list of masks. To do so, perform the following:
   a. Type the mask in the entry field.

**Examples of allowed file name masks:**

- *.txt - all files with the *.txt extension, for example, readme.txt or notes.txt;
- readme.?? - all files named readme with an extension of three characters, for example, readme.txt or readme.doc;
- test - all files named test without an extension.
b. Click the + button on the right of the entry field.

6. To delete a mask from the list of masks, highlight the mask entry in the list and click the X button.

7. To export the list of masks file:
   a. Click the button.
   b. In the window that opens, specify the file name in the File name field
   c. Click the Save button.

8. To import a list of masks from file:
   a. Click the button.
   b. In the window that opens, in the File name field specify the file containing the list of masks.
   c. Click the Open button.

9. Click the Save button.

**CONFIGURING SCANNING OF ATTACHED CONTAINERS AND ARCHIVES**

Kaspersky Security scans attached archives and containers by default. You can disable scanning of attachments or limit the nesting level of such objects to optimize the operation of Kaspersky Security, decrease the server load, and decrease mail traffic processing time. It is not recommended that you disable scanning of attachments for a long time, since they may contain viruses and other malicious objects.

To configure scanning of attached containers and archives:

1. Perform the following steps in the Administration Console tree:
   - To configure scanning of attached containers and archives for an unassigned Security Server, maximize the node of the relevant Security Server
   - To configure scanning of attached containers and archives for Security Servers belonging to a profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to configure scanning.

2. Select the Server protection node.

3. In the workspace, select the Advanced Anti-Virus settings tab.

4. Enable / disable scanning of attached containers and archives by performing one of the following actions:
   - If you want the application to scan such objects, select the Scan attached containers / archives with nesting level not higher than N check box.
   - If you want the application to ignore such objects, clear this check box.

5. Specify the allowed nesting level for attached containers and archives in the spin box.

6. Click the Save button.

If the application is running on a Microsoft Exchange DAG, the settings for scanning of attached containers and archives configured on one of the servers will be automatically applied to all servers within the DAG. Configuring scanning of attached containers and archives on other servers of the DAG is not necessary.

**CONFIGURING BACKGROUND SCAN SETTINGS**

If the application is running on a Microsoft Exchange DAG, the background scanning settings configured on one of the servers will be automatically applied to all servers within the DAG. Configuring background scanning settings on other servers of the DAG is not necessary.
To define the background scanning settings, perform the following steps:

1. Perform the following steps in the Administration Console tree:
   - To configure background scan settings for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To configure background scan settings for Security Servers belonging to a profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to configure background scan settings.

2. Select the Server protection node.

3. On the Protection for Mailbox role tab in the workspace, expand the Protection for mailboxes section.

4. In the Background scan section, use the Schedule drop-down list to select the option that suits you best:
   - Manually. Background scanning will have to be started manually.
   - Daily. Background scanning will be performed daily. Specify precise scan time in the entry field in <HH:MM> format.
   - On selected day. Background scanning will be performed on the selected days. Select check boxes opposite the days of the week when you would like to perform a background scan and specify the precise start time for the background scan in <HH:MM> format in the entry field.
   - Monthly. Background scanning is performed once a month. In the spin box, specify the day of the month when you would like to start a background scan and specify the precise start time for the background scan in <HH:MM> format in the entry field.

5. To have the application scan the message body during background scanning, select the Scan message content check box.

6. If you want the application to scan messages received over a specified time interval before the background scan start, select the Scan recent messages only check box and specify a number of days in the Scan messages received no later than <N> days before background scan spin box.

   This setting becomes more important in a configuration with a Microsoft Exchange 2013 server. The application performs background scanning of messages and other Microsoft Exchange objects that have been modified (including received ones) over N days preceding the start of a background scan.

   Maximum parameter value is 364 days.

7. Select the Limit the scan time check box and define the necessary value for the Stop the scan in <N> hours after scan start setting to optimize the scan duration.

8. Click the Save button.

9. To launch a background scan of a Microsoft Exchange server right away, click the Start scan button.

   Background scanning starts within a minute of the button click.

   Background scanning can be launched only on the Microsoft Exchange server on which the selected Security Server is installed. This remains true for any configuration of Microsoft Exchange servers, including DAG. For immediate launch of background scanning on other DAG servers, the background scan must be started separately for each Microsoft Exchange server.

10. To stop the background scan of a Microsoft Exchange server, click the Stop button.

    Background scanning stops within one minute of the button click.
PROTECTION AGAINST SPAM AND PHISHING

This section contains information about Anti-Spam and Anti-Phishing filtering of email traffic and instructions on configuring it.

In this section:
- About Anti-Spam protection .......................................................... 80
- About additional services, features, and anti-spam technologies .......................................................... 82
- Improving the accuracy of spam detection on Microsoft Exchange 2013 servers .......................................................... 83
- About anti-phishing scans .......................................................... 83
- Enabling and disabling Anti-Spam protection of the server .......................................................... 83
- Enabling and disabling message scanning for phishing .......................................................... 84
- Configuring spam and phishing scan settings .......................................................... 84
- Configuring the white and black lists of senders .......................................................... 86
- Configuring the white list of recipients .......................................................... 87
- Configuring an increase in the spam rating of messages .......................................................... 88
- Using external anti-spam message scanning services .......................................................... 90
- Configuring additional settings of spam and phishing scans .......................................................... 91

About Anti-Spam Protection

A key feature of Kaspersky Security is filtering out spam from the mail traffic passing through the Microsoft Exchange server. The Anti-Spam module filters incoming mail before messages reach user mailboxes.

Anti-Spam scans the following types of data:
- Internal and external traffic via SMTP using anonymous authentication on the server.
- Messages arriving on the server through anonymous external connections (edge server).

Anti-Spam does not scan the following types of data:
- Internal corporate mail traffic.
- External mail traffic arriving on the server during authenticated sessions. You can enable scanning of such mail traffic manually (see section "Configuring additional settings of spam and phishing scans" on page 91) using the Scan authorized connections setting.
- Messages arriving from other servers of the Microsoft Exchange mail infrastructure, because connections between servers within the same Microsoft Exchange infrastructure are considered to be trusted. Notably, if messages arrive in the infrastructure via a server on which Anti-Spam is inactive or not installed, the messages are not scanned for spam on all subsequent servers of this infrastructure along the path traveled by messages. You can enable scanning of such messages manually (see section "Configuring additional settings of spam and phishing scans" on page 91) using the Scan authorized connections setting.

Anti-Spam scans the message header, contents, attachments, design elements, and other message attributes. While performing the scan, Anti-Spam uses linguistic and heuristic algorithms that involve comparing the message being scanned with sample messages, as well as additional cloud services, such as Kaspersky Security Network (see section "About participation in Kaspersky Security Network" on page 72).
After filtering, Anti-Spam assigns one of the following statuses to messages:

- **Spam.** The message shows signs of spam.
- **Potential spam.** The message shows signs of spam but its spam rating is not high enough to mark it as spam.
- **Mass mailing.** A message belongs to a mass mailing (usually a news feed or advertisement) that lacks sufficient attributes for a spam verdict.
- **Formal notification.** An automatic message informing, for example, about mail delivery to the recipient.
- **Clean.** The message shows no signs of spam.
- **Blacklisted.** The sender's email address or IP address is on the black list of addresses.

You can choose actions to be taken by the application on messages with a specific status (see section "Configuring spam and phishing scan settings" on page 84). The following operations are available for selection:

- **Allow.** The message is delivered to recipients unchanged.
- **Reject.** An error message is returned to the sending server (error code 500), and the message is not delivered to the recipient.
- **Delete.** The sending server receives a notification that the message has been sent (code 250), but the message is not delivered to the recipient.
- **Add SCL value.** The application will assign a rating to messages indicating the probability of spam content inside (SCL, Spam Confidence Level). The SCL rating is a number ranging from 1 to 9. A high SCL rating means a high probability that the message is spam. The SCL rating is calculated by dividing the spam rating of the message by 10. If the resulting value exceeds 9, the SCL rating is assumed to equal 9. The SCL rating of messages is taken into account during subsequent processing of messages by the Microsoft Exchange infrastructure.
- **Add label to message header.** Messages that have been labeled as Spam, Potential spam, Mass mailing or Blacklisted are marked with special tags in the message subject: [!!SPAM], [!!Probable Spam], [!!Mass Mail] or [!!Blacklisted], respectively. You can edit the text of these tags (see section "Configuring spam and phishing scan settings" on page 84).

The application supports four sensitivity levels of anti-spam scanning:

- **Maximum.** This sensitivity level should be used if you receive spam very often. When you select this sensitivity level, the frequency of false positives rises: i.e., useful mail is more often recognized as spam.
- **High.** When this sensitivity level is selected, the frequency of false positives decreases (compared to the Maximum level) and the scan speed increases. The High sensitivity level should be used if you receive spam often.
- **Low.** When this sensitivity level is selected, the frequency of false positives decreases (compared to the High level) and the scan speed increases. This Low sensitivity level provides an optimum combination of scanning speed and quality.
- **Minimum.** This sensitivity level should be used if you receive spam rarely.

By default, the application uses the Low sensitivity level of anti-spam protection. You can increase or reduce the sensitivity level (see the section "Configuring spam and phishing scan settings" on page 84). Depending on the sensitivity level and the spam rating assigned after the scan, a message can be labeled as Spam or Probable spam (see table below).

<table>
<thead>
<tr>
<th>SENSITIVITY LEVEL</th>
<th>POTENTIAL SPAM</th>
<th>SPAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum</td>
<td>60</td>
<td>75</td>
</tr>
<tr>
<td>High</td>
<td>70</td>
<td>80</td>
</tr>
<tr>
<td>Low</td>
<td>80</td>
<td>90</td>
</tr>
<tr>
<td>Minimum</td>
<td>90</td>
<td>100</td>
</tr>
</tbody>
</table>
ABOUT ADDITIONAL SERVICES, FEATURES, AND ANTI-SPAM TECHNOLOGIES

The application uses the following additional features, services, and technologies of Kaspersky Lab for more thorough anti-spam protection of email:

- **DNSBL (Domain Name System Block List).** This feature retrieves information from DNSBL servers containing public lists of IP addresses used by spammers.

- **SURBL (Spam URI Realtime Block List).** This feature retrieves information from SURBL servers containing public lists of links leading to online resources advertised by spammers. Thus, if a message contains an URL from that list of URLs, it is labeled as spam.

Lists of DNSBL and SURBL servers are updated from Kaspersky Lab update servers together with the Anti-Spam databases every five minutes. Responses from DNSBL and SURBL servers are taken into account when determining the spam rating of a message. A spam rating is an integer ranging from 0 to 100. During spam rating calculation, the application considers the weight assigned to each responding DNSBL and SURBL server. If the total rating of the servers that have responded exceeds 100, the spam rating of such a message will be increased by 100. If it is smaller than 100, the spam rating of the message will not be increased.

- **KSN (Kaspersky Security Network).** It is an infrastructure of online services that improve user protection, accelerate the response of Kaspersky Lab applications to new threats and new types of spam, and minimize the number of Anti-Spam false positives.

KSN is disabled by default (see section "About participation in Kaspersky Security Network" on page 72). To start using KSN, you have to accept the KSN Statement that governs the procedure for collecting information from the computer running Kaspersky Security.

- **Enforced Anti-Spam Updates Service.** The service providing quick updates to the Anti-Spam database. If the Enforced Anti-Spam Updates Service is enabled, the application will keep contacting the servers of Kaspersky Lab and updating the Anti-Spam database as soon as new spam descriptions become available on Kaspersky Lab servers. This approach helps improve the efficiency of Anti-Spam against new emerging spam.

To ensure proper functioning of the Enforced Anti-Spam Updates Service the following conditions are required:

- a constant Internet connection of the computer that hosts the Security Server;

- regular updates of the Anti-Spam database (recommended frequency: every five minutes).

- **Reputation Filtering.** A cloud-enabled reputation filtering service of additional message scanning that moves messages requiring additional scanning to a special temporary storage – Quarantine. During the specified period (50 minutes), the application scans the message again using additional information received from Kaspersky Lab servers (for example, from KSN). If the application has not marked the message as spam during this time, it allows the message to reach the recipient. Reputation Filtering increases the accuracy of spam detection and reduces the probability of Anti-Spam false positives.

To be able to use Reputation Filtering, you have to confirm your participation in the Kaspersky Security Network (KSN) and accept a special KSN Statement.

Messages that have been moved to Quarantine by Reputation Filtering but have not been labeled as spam are delivered to recipients after the 50-minute period expires even if the application is closed or paused.

- **Dynamic DNS client.** This feature detects the potential belonging of the sender's IP address to a botnet using reverse lookup of its DNS. This functionality can be used provided that the protected SMTP server is not serving any xDSL or dial-up users.

- **SPF (Sender Policy Framework) technology.** A technology that checks the sender's domain for signs of spoofing. Domains use SPF to authorize certain computers to send mail on their behalf. If a message sender is not included in the list of authorized senders, its spam rating will be increased.
IMPROVING THE ACCURACY OF SPAM DETECTION ON MICROSOFT EXCHANGE 2013 SERVERS

When the application is installed on a Microsoft Exchange 2013 server deployed in the Client Access Server (CAS) role only, an additional component is available in the list of components that can be installed: CAS Interceptor. This component is designed to improve the accuracy of spam detection. It is recommended for installation on all Microsoft Exchange 2013 servers deployed in the Client Access Server (CAS) role only. This component is installed automatically together with the Anti-Spam component on Microsoft Exchange 2013 servers deployed in the Mailbox role (if you choose to install Anti-Spam (see section "Step 4. Selecting application components and modules" on page 25).

ABOUT ANTI-PHISHING SCANS

Kaspersky Security can scan messages for phishing and malicious URLs.

Phishing URLs lead to fraudulent websites designed to steal personal data of users, such as bank account details. A phishing attack can be disguised, for example, as a message from your bank with a link to its official website. By clicking the link, you go to an exact copy of the bank’s website and can even see the bank site’s address in the browser, even though you are actually on a spoofed site. From this point forward, all of your actions on the site are tracked and can be used to steal your private data.

Malicious URLs lead to web resources designed to spread malware.

To protect Microsoft Exchange servers against phishing and malicious URLs, the application uses databases of URL addresses that have been labeled as phishing or malicious URLs by Kaspersky Lab. The databases are regularly updated and are included in the Kaspersky Security delivery kit.

While scanning messages for phishing and malicious URLs, the application analyzes not only URLs but also the message subject, contents, attachments, design features, and other message attributes. The scan also uses heuristic algorithms and requests to the Kaspersky Security Network (see section "About participation in Kaspersky Security Network" on page 72) (KSN) cloud service if the use of KSN is enabled in Anti-Spam settings (see section "Configuring spam and phishing scan settings" on page 84). With the help of KSN, the application receives the latest information about phishing and malicious URLs before they appear in Kaspersky Lab databases.

On detecting phishing or malicious URLs in a message, the application labels it as Phishing. You can choose actions to be taken by the application on messages with this status. The following operations are available for selection:

- **Allow**: The message is delivered to recipients unchanged.
- **Reject**: An error message is returned to the sending server (error code 500), and the message is not delivered to the recipient.
- **Delete**: The sending server receives a notification that the message has been sent (code 250), but the message is not delivered to the recipient.
- **Add SCL and PCL rating**: The application adds a spam confidence level (SCL) rating of 9 and a phishing confidence level (PCL) rating to 8 to messages. On arriving in the Microsoft Exchange mail infrastructure, messages with a high PCL rating (more than 3) are automatically directed to the Junk E-Mail folders, and all URLs contained in them are deactivated.
- **Add label to message header**: Messages with Phishing status are marked with a special [!!Phishing] label in the message subject. You can edit the text of this label tags (see section "Configuring spam and phishing scan settings" on page 84).

ENABLING AND DISABLING ANTI-SPAM PROTECTION OF THE SERVER

Disabling Anti-Spam protection of the server considerably increases the risk of unwanted email. We do not recommend disabling Anti-Spam protection unless absolutely necessary.
To enable or disable Anti-Spam protection of a Microsoft Exchange server:

1. Perform the following steps in the Administration Console tree:
   - To enable or disable Anti-Spam protection for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To enable or disable Anti-Spam protection for Security Servers belonging to a profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to configure Anti-Spam protection.
2. Select the Server protection node.
3. On the Protection for Hub Transport role tab in the workspace, perform one of the following actions in the Anti-Virus scan settings section:
   - To enable Anti-Spam protection, select the Enable anti-spam scanning of messages check box.
   - To disable Anti-Spam protection, clear the Enable anti-spam scanning of messages check box.
4. Click the Save button.

Enabling and Disabling Message Scanning for Phishing

You can enable Anti-Phishing scanning of messages only if Anti-Spam protection of the server is enabled. Anti-Phishing scanning also includes scanning for malicious URLs.

To enable or disable Anti-Phishing scanning of messages:

1. Perform the following steps in the Administration Console tree:
   - To enable or disable Anti-Phishing scanning of messages for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To enable or disable Anti-Phishing scanning of messages for Security Servers belonging to one profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to configure Anti-Phishing scanning.
2. Select the Server protection node.
3. On the Protection for Hub Transport role tab in the workspace, perform one of the following actions in the Anti-Virus scan settings section:
   - To enable Anti-Phishing scanning of messages, select the Enable anti-phishing scanning of messages check box.
   - To disable Anti-Phishing scanning of messages, clear the Enable anti-phishing scanning of messages check box.
4. Click the Save button.

Configuring Spam and Phishing Scan Settings

To configure the Anti-Spam and Anti-Phishing scanning settings:

1. Perform the following steps in the Administration Console tree:
   - To configure the Anti-Spam and Anti-Phishing scanning settings for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To configure the Anti-Spam and Anti-Phishing scanning settings for Security Servers belonging to a profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to configure the Anti-Spam and Anti-Phishing scanning settings.
2. Select the Server protection node.
3. On the Protection for Hub Transport role tab in the workspace, expand the Anti-Spam analysis settings section.
In the opposite the relevant parameters: box, configure the actions to be taken by the application on messages labeled as incoming mail for phishing links. Select the parameters:

- **Allow.** The message is delivered to recipients unchanged.
- **Reject.** An error message is returned to the sending server (error code 500), and the message is not delivered to the recipient.
- **Delete.** The sending server receives a notification that the message has been sent (code 250), but the message is not delivered to the recipient.

In the Spam processing settings configuration section, in the Action drop-down list select the action to be taken by the application on messages with each of the statuses mentioned (Spam, Probable spam, Mass mailing, Formal notification, Blacklisted):

- **Add SCL value.** The application will add a Spam Confidence Level score to the message (SCL score). The SCL score is a number ranging from 1 to 9. A high SCL score means a high probability that the message is spam. The SCL rating of messages is taken into account during subsequent processing of messages by the Microsoft Exchange infrastructure.

- **Save a copy.** A copy of the message can be saved in Backup.

- **Add label to message header.** Messages that have been labeled as Spam, Probable spam, Mass mailing or Blacklisted are marked with special tags in the message subject: [!!SPAM], [!!Probable Spam], [!!Mass Mail] or [!!Blacklisted], respectively. If necessary, edit the text of these tags in the entry fields corresponding to the statuses.

Select the Enable anti-phishing scanning of messages check box if you want the application to scan incoming mail for phishing links.

In the Spam processing settings section, under the Enable anti-phishing scanning of messages check box, in the Action drop-down list select the action to be taken by the application on messages labeled as Phishing:

- **Allow.** The message is delivered to recipients unchanged.
- **Reject.** An error message is returned to the sending server (error code 500), and the message is not delivered to the recipient.
- **Delete.** The sending server receives a notification that the message has been sent (code 250), but the message is not delivered to the recipient.

In the Spam processing settings section, under the Enable anti-phishing scanning of messages check box, configure the actions to be taken by the application on messages labeled as Phishing: Select check boxes opposite the relevant parameters:

- **Add SCL and PCL rating.** The application adds a spam confidence level (SCL) rating of 9 and a phishing confidence level (PCL) rating of 8 to messages. On arriving in the Microsoft Exchange mail infrastructure, messages with a high PCL rating (more than 3) are automatically directed to the Junk E-Mail folders, and all URLs contained in them are deactivated.

- **Save a copy.** A copy of the message can be saved in Backup.

- **Add label to message header.** Messages with Phishing status are marked using a special label in the message subject: [!!Phishing]. If necessary, edit the text of this label in the entry field on the right.

In the Spam processing settings section, configure the usage of additional spam scanning services (see section "About additional services, features, and anti-spam technologies" on page 82):

- To enable the use of KSN during anti-spam and anti-phishing scans:
  a. Select the Use Kaspersky Security Network (KSN) check box.
  b. If necessary, specify the timeout for requests to a KSN server in the Maximum timeout for a KSN request scroll field.

The default value is 5 sec.

The Use Kaspersky Security Network (KSN) check box is available when the I accept the KSN Statement check box is selected in the KSN settings section of the Settings node.
To enable the use of the Reputation Filtering service, select the **Use Reputation Filtering** check box.

To be able to use Reputation Filtering, you have to confirm your participation in the Kaspersky Security Network (KSN) and accept a special KSN Statement.

If you want the application to use the service for prompt delivery of Anti-Spam database updates, select the **Use Enforced Anti-Spam Updates Service** check box.

If you want the application to connect to the KSN and Enforced Anti-Spam Updates Service servers via a proxy server, select the **Use proxy to access KSN and Enforced Anti-Spam Updates Service** check box.

You can configure the proxy server settings in the Settings node (see section "Configuring the settings of the connection to the update source" on page 67).

12. Click the **Save** button.

## Configuring the White and Black Lists of Senders

You can configure two kinds of lists of senders:

- White lists contain addresses belonging to trusted senders whose messages should not be scanned for spam.
- Black lists contain addresses belonging to senders all of whose messages are labeled as spam.

Kaspersky Security supports white and black lists of email addresses and IP addresses.

### Configuring the White / Black Lists of Email Addresses of Senders

To configure the white / black lists of email addresses of senders:

1. Perform the following steps in the Administration Console tree:
   - To configure the white / black lists of email addresses of senders for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To configure the white / black lists of email addresses of senders for Security Servers belonging to a profile, maximize the **Profiles** node and inside it maximize the node of the profile for whose Security Servers you want to configure the lists.

2. Select the **Server protection** node.

3. On the **Protection for Hub Transport role** tab in the workspace, open the **Settings of Anti-Spam black and white lists** section.

4. Select the **Add sender’s address to white / black list** check box.

5. Add an email address to the list To do so, perform the following:
   a. Type the email address in the entry field. You can specify an individual e-mail address or a mask, such as *@domain.com, covering all addresses of a specific email domain.
   b. Click the **+** button.

6. To remove an email address from the list, select an address in the list and click the **X** button.

7. To export the list to a file, click the **-export** button.

8. To import the list from a file, click the **-import** button.

9. Click the **Save** button.

### Configuring the White / Black Lists of IP Addresses of Senders

To configure the white / black lists of IP addresses of senders:

1. Perform the following steps in the Administration Console tree:
   - To configure the white / black lists of IP addresses of senders for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To configure the white / black lists of IP addresses of senders for Security Servers belonging to a profile, maximize the **Profiles** node and inside it maximize the node of the profile for whose Security Servers you want to configure the lists.
2. Select the **Server protection** node.

3. On the **Protection for Hub Transport role** tab in the workspace, open the **Settings of Anti-Spam black and white lists** section.

4. Select the **Add sender's address to white / black list of IP addresses** check box.

5. To add an IP address to the list:
   a. Type the IP address in the entry field. You can specify a solitary IP address or a range of IP addresses in CIDR notation (represented as XXX.XXX.XXX.XXX/YY).
   b. Click the **+** button.

6. To remove an IP address from the list, select it in the list and click the **X** button.

7. To export the list to a file, click the **Export** button.

8. To import the list from a file, click the **Import** button.

9. Click the **Save** button.

### Configuring the White List of Recipients

You can configure the **white list of recipients** by adding or removing addresses of message recipients. Messages for recipients added to that list will not be checked for spam presence. The white list is empty by default.

You can add recipients' addresses to the white list in the form of entries of the following types:

- **Active Directory objects**:
  - User.
  - Contact.
  - Distribution Group.
  - Security Group.

It is recommended to add addresses to the white list in the form of objects of this type.

- **SMTP addresses** in the `mailbox@domain.com` format. Entries of this type should be added if the address you want to exclude cannot be located in Active Directory.

To exclude a public folder from scanning for spam, you should add all of its SMTP addresses (if there are several of them) to the white list. If any of the SMTP addresses of the public folder are not on the list, messages arriving in the public folder can be scanned.

Recipients' addresses specified in the form of Active Directory objects are excluded from the anti-spam scan according to the following rules:

- If the recipient's address is specified as a User or a Contact, messages addressed to this recipient are excluded from scanning.
- If the address is specified as a Distribution Group, messages addressed to this distribution group are excluded from the scan. However, messages addressed personally to individual distribution group members are not excluded from the scan unless their addresses have been added to the list separately.
- If the address is specified as a Security Group, messages addressed to this group and its members are excluded from the scan. However, if a nested security group is a member of the specified Security Group, messages addressed to members of the nested security group are not excluded from the scan unless their addresses have been added to the list separately.

The application automatically updates user addresses received from Active Directory following changes to the relevant Active Directory accounts (for example, when a user's email address has changed or a new member has been added to a security group). This update is performed once a day.

**the white list of recipients:**

1. Perform the following steps in the Administration Console tree:
   - To configure the white list of recipients for an unassigned Security Server, maximize the node of the relevant Security Server;
To configure the white list of recipients for Security Servers belonging to a profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to configure the white list of recipients.

2. Select the Server protection node.

3. On the Protection for Hub Transport role tab in the workspace, open the Settings of Anti-Spam black and white lists section.

4. Select the Add recipient’s address to white list check box.

5. Add the recipient's address to the white list of recipients. To do so, perform the following:

   To add an Active Directory account to the list:
   a. Click the button.
   b. In the window that opens, locate the relevant Active Directory account and click OK.

   Addresses selected in Active Directory are marked in the list by the following symbols:
   - users, contacts, distribution groups;
   - security groups.

   To add an SMTP address or a public folder to the list:
   - To add an SMTP address, type it in the entry field and click the button.
   - To add a public folder, enter the path to the folder and click the button.

   Addresses added in this way are marked with the icon.

   Addresses added in this way are not checked for their presence in Active Directory.

6. To remove an address from the list, select an entry and click the button.

7. To export the list to a file, click the button.

8. To import the list from a file, click the button.

9. Click the Save button.

**Configuring an Increase in the Spam Rating of Messages**

You can configure the Anti-Spam settings affecting detection of a special message property - its spam rating. These settings allow you to configure the application to increase the spam rating of a message based on the analysis of its sender’s email address and message subject, as well as when the message is written in a foreign language.

To configure the application to increase the spam rating of a message based on the analysis of its sender’s address:

1. Perform the following steps in the Administration Console tree:
   - To configure the application to increase the spam rating of messages for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To configure the application to increase the spam rating of messages for Security Servers belonging to a profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to configure the application to increase the spam rating of messages.

2. Select the Server protection node.

3. On the Protection for the Hub Transport role tab in the workspace, open the Spam rating detection settings section.
4. In the **Increase spam rating if**: configuration section, select the check boxes for the following settings as necessary:
   - **The "To" field contains no addresses.** The spam rating of a message will be increased if its "To" field is empty.
   - **The sender’s address contains numbers.** The spam rating of a message will be increased if the address of its sender contains digits.
   - **Sender’s address in the message body does not contain the domain part.** The spam rating of a message will be increased if the address of its sender contains no domain name.

5. Click the **Save** button.

**To configure the application to increase the spam rating of messages based on the analysis of the message subject:**

1. Perform the following steps in the Administration Console tree:
   - To configure the application to increase the spam rating of messages for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To configure the application to increase the spam rating of messages for Security Servers belonging to a profile, maximize the **Profiles** node and inside it maximize the node of the profile for whose Security Servers you want to configure the application to increase the spam rating of messages.

2. Select the **Server protection** node.

3. On the **Protection for the Hub Transport role** tab in the workspace, open the **Spam rating detection settings** section.

4. In the **Increase spam rating if the subject contains**: configuration section, select check boxes for the following settings as necessary:
   - **More than 250 characters.** The spam rating of a message will be increased if its subject contains more than 250 characters.
   - **Many blanks and/or dots.** The spam rating of a message will be increased if its subject contains multiple spaces and / or dots.
   - **Time stamp.** The spam rating of a message will be increased if its subject contains a digital ID or a time stamp.

5. Click the **Save** button.

**To configure the application to increase the spam rating of messages based on the analysis of its content language:**

1. Perform the following steps in the Administration Console tree:
   - To configure the application to increase the spam rating of messages for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To configure the application to increase the spam rating of messages for Security Servers belonging to a profile, maximize the **Profiles** node and inside it maximize the node of the profile for whose Security Servers you want to configure the application to increase the spam rating of messages.

2. Select the **Server protection** node.

3. On the **Protection for the Hub Transport role** tab in the workspace, open the **Spam rating detection settings** section.

4. In the **Increase spam rating if message language is**: configuration section, select the check boxes for the languages whose presence in a message you consider to be a sign of spam:
   - **Chinese**, if you are not expecting mail in the Chinese language.
   - **Korean**, if you are not expecting mail in the Korean language.
   - **Thai**, if you are not expecting mail in the Thai language.
   - **Japanese**, if you are not expecting mail in the Japanese language.

5. Click the **Save** button.
USING EXTERNAL ANTI-SPAM MESSAGE SCANNING SERVICES

To ensure more thorough Anti-Spam filtering of email messages, you can enable the use of external services (see section “About additional services, features, and anti-spam technologies” on page 82).

To enable the use of external services to check IP addresses and URLs for spam:

1. Perform the following steps in the Administration Console tree:
   - To configure the use of external anti-spam message scanning services for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To configure the use of external anti-spam message scanning services for Security Servers belonging to a profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to configure the use of external anti-spam message scanning services.

2. Select the Server protection node.

3. On the Protection for Hub Transport role tab in the workspace, open the Using external Anti-Spam services section.

4. Select the Use external anti-spam analysis services check box if you want the application to consider the IP address and URL scan results of these services during anti-spam analysis.

5. If you want the application to scan messages for spam based on the default DNSBL black list, select the Use default black list of the DNSBL service check box in the DNSBL configuration section.

6. To use a custom list of DNS names of servers and assign other weight coefficients to them, select the Use a different list from the black list set of the DNSBL service check box. When this check box is selected, the option allows you to create a custom list below. To do so, perform the following:
   - To add an entry to the custom list, specify the DNS name of the server and its weight coefficient in the corresponding fields and click the button.
   - To delete an entry from the custom list, click the button.
   - To import a custom list, click the button.
   - To export a custom list, click the button.

7. If you want the application to scan messages for spam based on the default SURBL black list, select the Use default black list of the SURBL service check box in the SURBL configuration section.

8. To use a custom list of DNS names of servers and assign other weight coefficients to them, select the Use a different list from the black list set of the SURBL service check box. When this check box is selected, the option allows you to create a custom list below. To do so, perform the following:
   - To add an entry to the custom list, specify the DNS name of the server and its weight coefficient in the corresponding fields and click the button.
   - To remove a record, click the button.
   - To import a custom list, click the button.
   - To export a custom list, click the button.

9. To enable a reverse DNS lookup of the sender’s IP address, select the Check sender IP for presence in DNS check box.

10. To enable the use of SPF technology, select the Check SPF record check box.

11. If you want the application to check if the sender’s IP address belongs to a botnet based on its reverse DNS zone, select the Check if sender’s IP address is dynamic check box.

12. In the Maximum DNS request timeout spin box, enter the maximum time in seconds.

The default value is 5 sec. After timeout, the application scans the message for spam without checking if the sender’s IP address belongs to a dynamic DNS.
CONFIGURING ADDITIONAL SETTINGS OF SPAM AND PHISHING SCANS

You can configure additional Anti-Spam and Anti-Phishing analysis settings, such as time- or size-based scanning restrictions, and spam analysis of Microsoft Office files attached to messages.

To configure time- or size-based Anti-Spam and Anti-Phishing scanning restrictions:

1. Perform the following steps in the Administration Console tree:
   - To configure Anti-Spam and Anti-Phishing scanning restrictions for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To configure Anti-Spam and Anti-Phishing scanning restrictions for Security Servers belonging to a profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to configure Anti-Spam and Anti-Phishing scanning restrictions.
2. Select the Server protection node.
3. On the Protection for Hub Transport role tab in the workspace, open the Advanced settings of Anti-Spam section.
4. In the Restrictions section, use the Maximum time for scanning a message spin box to specify the necessary value in seconds.
   - If the message scan duration exceeds the specified time, the Anti-Spam or Anti-Phishing scan of the message stops. The default value is 60 sec. If the application is configured to add service headers to the message, they will contain information to the effect that the maximum scan time has been exceeded.
5. In the Restrictions configuration section, use the Maximum object size to scan spin box to specify the necessary value in kilobytes.
   - If the message with all attachments exceeds the specified size, Anti-Spam and Anti-Phishing scanning is not performed, and the message is delivered to the recipient. The default value is 1,536 KB (1.5 MB). The maximum value is 20 MB, and the minimum value is 1 KB. If the application is configured to add service headers to the message, they will contain information to the effect that the maximum object size has been exceeded.
6. Click the Save button to save the changes.

To configure the settings of Anti-Spam and Anti-Phishing scanning of Microsoft Office files:

1. Perform the following steps in the Administration Console tree:
   - To configure the settings of Anti-Spam and Anti-Phishing scanning of Microsoft Office files for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To configure the settings of Anti-Spam and Anti-Phishing scanning of Microsoft Office files for Security Servers belonging to a profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to configure the settings of Anti-Spam and Anti-Phishing scanning of Microsoft Office files.
2. Select the Server protection node.
3. On the Protection for Hub Transport role tab in the workspace, open the Advanced settings of Anti-Spam section.
4. In the Scan settings for Microsoft Office files configuration section, perform the following steps:
   - If you want the application to scan Microsoft Word documents for spam and phishing links, select the Scan DOC files check box.
   - If you want the application to scan RTF documents for spam and phishing links, select the Scan RTF files check box.
5. Click the Save button to save the changes.

To configure additional Anti-Spam and Anti-Phishing scan settings:

1. Perform the following steps in the Administration Console tree:
   - To configure additional Anti-Spam and Anti-Phishing scan settings for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To configure additional Anti-Spam and Anti-Phishing scan settings for Security Servers belonging to a profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to configure additional Anti-Spam and Anti-Phishing scan settings.
2. Select the **Server protection** node.

3. On the **Protection for Hub Transport role** tab in the workspace, open the **Advanced settings of Anti-Spam** section.

4. If you want the application to analyze images in mail attachments using image analysis technology (GSG), select the **Use image analysis** check box.
   
   It is used to analyze images by checking them against the samples in the Anti-Spam database. If a match is found, the spam rating of such messages will be increased.

5. If you want the application to add X-headers to messages containing information about the scan results, select the **Enable service headers** check box.

6. Select the **Scan authorized connections** check box to enable scanning of mail received via a trusted connection for spam and phishing.

7. Select the **Skip messages for the Postmaster address** check box to disable scanning of messages arriving for the Postmaster address for spam and phishing.

8. Click the **Save** button to save the changes.
This section contains information about Backup and how to use it.

**IN THIS SECTION:**

- About Backup
- Viewing the Backup contents
- Viewing properties of objects in Backup
- Filtering the list of Backup objects
- Saving objects from Backup to disk
- Sending an objects from Backup to recipients
- Deleting objects from Backup
- Configuring Backup settings
- Selecting Backup database for viewing its contents from the profile

---

**ABOUT BACKUP**

Before processing messages, Kaspersky Security moves copies of messages to Backup. Copies of messages are placed in Backup together with all attachments.

Kaspersky Security places copies of messages in Backup in the following cases:

- After message scanning by the Anti-Virus module, before modifying the message by Delete message or Delete object operations, provided that the application is configured to move copies of messages to Backup during Anti-Virus scanning (see section "Configuring object processing settings" on page 74).
- After scanning messages for spam and phishing, before performing the Delete or Reject operations on the message, provided that the application is configured to move copies of messages to Backup during spam and phishing scans (see section "Configuring spam and phishing scan settings" on page 84).

You can manage copies of messages in Backup as follows:

- View the contents of Backup (see section "Viewing the Backup contents" on page 94).
- View the details of messages in Backup (see section "Viewing the properties of objects in Backup" on page 94).
- Filter the details of messages in Backup for convenient viewing and searching of message details (see section "Filtering the list of Backup objects" on page 95).
- Save messages from Backup to disk in order to view information contained in the message (see section "Saving objects from Backup to disk" on page 96). You can also attempt to rescan the saved message with Anti-Virus with the updated database.
- Deliver messages from Backup to recipients (see section "Delivering messages from Backup to recipients" on page 96). Saved objects will be delivered to the recipients.
- Delete message copies from Backup (see section "Deleting objects from Backup" on page 96).

Information about Backup objects is stored in the SQL database specified during installation of the application (see section "Step 5. Setting up the application's connection to the database of Backup and statistics" on page 26). If several Security Servers use the same SQL database (for example, in a DAG server configuration), Backup stores messages received from each of these Security Servers.

Messages are stored in Backup in encrypted form, which eliminates the risk of infection and speeds up the operation of Anti-Virus (files in Backup format are not detected as infected).

The total number of objects in Backup is limited to one million. You can additionally limit Backup size by restricting Backup size and object storage duration (see section "Configuring Backup" on page 97).
The application checks every minute if these limitations are not exceeded. Based on the results of the check, the application can perform the following operations:

- If the allowed number of objects in Backup is exceeded, the application removes an appropriate quantity of the oldest objects.
- If there is a limit on Backup size in megabytes, and this limit is exceeded when a new message is moved to Backup, the application frees up the required space by deleting the oldest objects.
- If the message storage period is limited, the application deletes messages whose storage period has expired.

**VIEWING THE BACKUP CONTENTS**

You can view the details of all objects stored in Backup (copies of messages and attachments).

*To view the Backup content, perform the following steps:*

1. In the Administration Console tree, expand the node of a Security Server.
2. Select the **Backup** node.

The workspace shows a table with information about objects saved in Backup.

The lower part of the workspace under the table shows the total number of objects in Backup, the space occupied by them, and the number of objects displayed in the workspace after a filter was applied.

By default, the table shows the following details of each object in Backup:

- **From.** The e-mail address of the message sender.
- **To.** The e-mail address of the message recipient.
- **Subject.** Message subject.
- **Status.** Object scan status (Infected, Probably infected, Disinfected, Spam, Probable spam, Mass mailing Phishing, Blacklisted, Formal notification, Trusted, Protected, Corrupted, No access, Not found, Scanning timeout, Scanning in progress, Scan error).
- **Reception date.** Precise time of message arrival on Microsoft Exchange server.

You can set up the appearance of the workspace by editing the table columns displayed and changing their order.

*To set up the appearance of the workspace:*

1. Click the **Select columns** button to add or remove table columns.
2. In the window that opens, perform the following operations:
   - Select the check boxes next to the table columns that you want to view in the workspace.
   - Clear the check boxes for the table columns that you want to hide.

You can sort table data by any table column by clicking the header of the relevant column, such as **From**, **To**, or **Subject**.

The number of objects that the workspace can display at any one time is limited. To view other objects, use the navigation buttons in the bottom right corner of the workspace. The current window number is displayed between the two pairs of navigation buttons. To proceed to the next window, click the button with the > symbol. To proceed to the previous window, click the button with the < symbol. To proceed to the last window, click the button with the >> symbol. To return to the first window, click the button with the << symbol.

**VIEWING PROPERTIES OF OBJECTS IN Backup**

*To view the properties of an object in Backup:*

1. In the Administration Console tree, expand the node of a Security Server.
2. Select the **Backup** node.
3. In the table listing Backup objects in the workspace, select the object (message or attachment) of which you want to view the properties.
4. Click the **Properties** button in the upper part of the workspace above the list of objects.
The **Message properties** window opens. You can view the following details in this window:

- **Virus.** The virus name will appear in this field if a message is infected.
- **Object type.** Object type: message, message body, or attachment.
- **From.** The sender's address.
- **To.** The e-mail address of the message recipient.
- **Copy.** Address of the message copy recipient.
- **Object name.** Name of the message or attachment file.
- **Size on disk.** Disk space occupied by the message.
- **Subject.** Message subject.
- **Path.** Object storage path.
- **Server name.** Name of the server that has placed the object in Backup.
- **Received.** Precise time of message delivery (day, month, year, hour, minute).
- **Sent.** Exact time when the message was sent (day, month, year, hour, minute).
- **Release date of the databases.** Release date of the databases.
- **Status.** Status assigned by the application to a message.
- **Size.** Size of an object (message or attachment) in bytes.

You can select several objects and view their status information.

> **To view the properties of several objects in Backup:**

1. In the Administration Console tree, expand the node of a Security Server.
2. Select the **Backup** node.
3. In the table listing Backup objects in the workspace, select the objects of which you want to view the properties.
4. Click the **Properties** button in the upper part of the workspace above the list of objects.

The **Properties of the selected objects** window opens. This window lets you view the status of all selected objects and the number of selected objects with a particular status.

**Filtering the list of Backup objects**

You can filter the list of Backup objects using one or several conditions by means of the filter. Filtering conditions are applied to table columns. By adding conditions, you can create custom filters. Filtering conditions are combined using the “AND” logical operator. Backup objects that do not meet the filtering conditions are not displayed in the list.

> **To filter the list of Backup objects:**

1. In the Administration Console tree, expand the node of a Security Server.
2. Select the **Backup** node.
3. Configure the filtering conditions in the **Storage filter** section:
   a. Select the column to which the condition should be applied in the drop-down list.
      Depending on the column selected, the remaining condition parameters may take the following form:
      - Drop-down list
      - Drop-down list and entry field
   b. Select the setting value(s) in the drop-down list and/or enter them manually.
4. If necessary, specify additional criteria by clicking the **Add a condition** button. Remove unnecessary conditions by clicking the **X** button in the right part of the row with the condition.
5. Click the **Apply filter** button to filter the list of Backup objects.

The application displays Backup objects matching the filter conditions in the table. Backup objects that do not match the filter conditions are hidden.
Once filter is applied, you can also sort table data in ascending or descending order by any table column. To do so, click the header of a particular column, for example From, To, or Subject.

**SAVING OBJECTS FROM BACKUP TO DISK**

Saving objects from Backup may cause the computer to be infected.

To save an object from Backup to disk:

1. In the Administration Console tree, expand the node of a Security Server.
2. Select the Backup node.
3. In the table listing Backup objects in the workspace, select the object that you want to save.
4. Click the Save to disk button in the upper part of the workspace above the list of objects.
5. In the window that opens, specify the folder to which you wish to save the object and, if necessary, enter or modify the object name.
6. Click the Save button.

The application will decode the encrypted object and save its copy with the defined name in the specified folder. The saved object has the same format that it had before being processed by the application. After an object has been saved successfully, the application displays the following notification: "Selected object has been saved to disk".

**SENDING AN OBJECTS FROM BACKUP TO RECIPIENTS**

You can send a copy of a message saved in Backup to its original recipients.

The addresses of the message recipients must be added to the list of trusted recipients in Anti-Virus (see the section "Configuring exclusions by addresses of recipients" on page 76). Otherwise, sending the message may be blocked, and the message may be returned to Backup.

To send an object from Backup to recipients, perform the following steps:

1. In the Administration Console tree, select the node of a Microsoft Exchange server and open it.
2. Select the Backup node.
3. In the table listing Backup objects in the workspace, select the message that you want to send to recipients.
4. Click the Send to recipients button in the upper part of the workspace above the list of objects.

The application sends the selected object to the recipients of the original message.

**DELETING OBJECTS FROM BACKUP**

The application deletes the following objects from Backup automatically:

- The oldest object, if adding a new object will cause the limit on the total number of objects in Backup to be exceeded (the maximum number of files in this version is limited to one million).
- The oldest object, if there is a limit on the size of Back and adding a new object will cause this limit to be exceeded.
- Objects whose storage period has expired, if there is a restriction imposed on the storage period.

Objects may also be manually removed from Backup storage. This feature may prove useful for deleting objects that have been saved to disk, and to free up space in Backup.

To delete objects from Backup:

1. In the Administration Console tree, select the node of a Microsoft Exchange server and open it.
2. Select the Backup node.
3. In the table listing Backup objects in the workspace, select the object(s) that you want to delete. You can use a filter to search for objects (see section "Filtering the list of Backup objects" on page 95).

4. Click the **Delete** button in the lower part of the workspace.

   A confirmation window opens.

5. Click **Yes** in the confirmation window.

   The application deletes selected objects from Backup.

To delete all objects from Backup:

1. In the Administration Console tree, select the node of a Microsoft Exchange server and open it.
2. Select the **Backup** node.
3. Click the **Delete all** button in the workspace.

   A confirmation window opens.

4. Click **Yes** in the confirmation window.

   If filters have been applied to Backup content, the application removes from Backup only the objects matching the filters. If filters have not been applied to Backup content, the application removes all objects from Backup.

**CONFIGURING BACKUP SETTINGS**

Backup is created during installation of the Security Server. Backup settings have default values that can be modified by the administrator.

To change the Backup settings, perform the following steps:

1. In the Administration Console tree, select the node of a Microsoft Exchange server and open it.
2. Select the **Settings** node.
3. To limit the size of Backup:
   - In the workspace, in the **Data storage** section, select the **Limit Backup size** check box.
   - Specify the maximum allowed Backup size in the **Backup size may not exceed** spin box.
   
   The default maximum size of Backup is 5,120 MB.
4. To limit the duration of object storage in Backup:
   - In the workspace, in the **Data storage** section, select the **Limit duration of objects storage in Backup** check box.
   - Specify the number of days in the **Store objects no longer than** spin box.
   
   The default period of object storage in Backup is limited to 45 days.
5. Click the **Save** button.

   If not a single check box is selected in the **Data storage** configuration section, only the total number of Backup objects is limited (not to exceed 1 million objects).

Regardless of the application configuration (standalone server or DAG), Backup settings have to be configured separately on each physical server.

**SELECTING BACKUP DATABASE FOR VIEWING ITS CONTENTS FROM THE PROFILE**

Information about Backup objects is stored in the SQL database specified during installation of the application (see section "Step 5. Setting up the application's connection to the database of Backup and statistics" on page 26).

When several Security Servers have been added to a profile, by default the node of the profile shows the node of the Backup whose SQL database server appears first in the list arranged alphabetically in the format `<SQL server name>\<instance>`.
In the profile, you can select the SQL database to store information about Backup objects in the storage whose contents you want to view.

To select a Backup database in the profile to view its contents:

1. In the Administration Console tree, expand the Profiles node.
2. Expand the node of the profile containing the Security Server that uses the relevant SQL database.
3. Select the Backup node.
4. In the workspace, click the Select button.

   The Database window opens, listing all SQL databases that are used by at least one Security Server in the profile.

5. In the Database window, select the Security Server that hosts the SQL database of the Backup you need.
6. Click OK.

If the connection is to a remote database on an SQL server, make sure that this SQL server is enabled to support TCP/IP as a client protocol.
DATA LEAK PREVENTION

This section provides information and instructions on how to implement prevention of confidential data leaks via corporate email.

In this section:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About data leak prevention</td>
<td>99</td>
</tr>
<tr>
<td>Managing the DLP Module</td>
<td>99</td>
</tr>
<tr>
<td>Enabling and disabling Data Leak Prevention</td>
<td>100</td>
</tr>
<tr>
<td>Assigning the DLP query controller server</td>
<td>100</td>
</tr>
<tr>
<td>Configuring the connection to the DLP database</td>
<td>101</td>
</tr>
</tbody>
</table>

About data leak prevention

Kaspersky Security 9.0 for Microsoft Exchange Servers includes a data leak prevention (DLP) component – the DLP Module. The DLP Module analyzes messages for any confidential information or data with specific parameters, such as bank card details, financial or personal data of company employees. If DLP Module detects such information in a message, it adds to the DLP database (see the section "Managing DLP Module" on page 99) a record of information security violation (incident). This record helps to determine who attempted to send information and where to. The DLP Module can either block transmission of messages with confidential information or allow them and only reflect the fact of data transmission in the DLP database.

The DLP Module detects violations of data security on the basis of DLP categories (hereinafter referred to as categories) and DLP policies (hereinafter referred to as policies).

Configuring categories and policies, as well as processing incidents, make part of the working duties of an information security specialist. An information security specialist is a user of the application to whom the corresponding role has been assigned (see the section "Role-based access" on page 56). The tasks of an information security specialist and instructions on how to accomplish them are provided in the Kaspersky Security 9.0 for Microsoft Exchange Servers Information Security Specialist's Guide.

The application allows the joint work of several security officers. All the controls and features of DLP Module are available to any user who has been assigned the Information Security Specialist role. All of the controls and features of DLP Module are available for any user who has been assigned the Information Security Specialist role.

If the law in your country requires notifying individuals that their activity on data transmission networks is being monitored, you must warn users about the operation of the DLP Module in advance.

Managing the DLP Module

Acting as the application administrator, you can activate and deactivate the DLP Module in your organization, as well as redefine its settings, such as the settings of the DLP query server controller and the settings for connection to the DLP database. Kaspersky Security allows managing those settings in centralized mode for the entire organization without having to switch between different Security Servers and configure the DLP Module on each Security Server individually.

DLP query controller server

One of the security Servers with DLP Module installed at the organization is the DLP query controller server. This Security Server performs tasks related to preventing data leaks such as the creation of categories or the drawing up of reports. All requests from Administration Consoles of security officers are processed by this server.

By default, the DLP query controller server is the first corporate Security Server on which the DLP Module was installed during application installation or upgrade. You can assign (see section "Assigning the DLP query controller server" on page 100) another Administration Server with the DLP Module installed as a DLP query controller server.
DLP database

The application saves data on categories, policies, and incidents in the dedicated SQL database – the DLP database. The DLP database can be stored locally, on the same computer with Security Server, or on a remote computer on an organization’s network (see the section “Configuring connection to the DLP database” on page 101).

Kaspersky Security does not encrypt data transmitted between the Security Server and the DLP database. When the DLP database is hosted on a remote computer, you have to manually encrypt data transmitted via communication channels if such encryption is required by the information security policy of your company.

ENABLING AND DISABLING DATA LEAK PREVENTION

By default, Data Leak Prevention is enabled after the application is installed. We do not recommend disabling Data Leak Prevention unless absolutely necessary. You are advised to request permission to disable Data Leak Prevention from the security officer.

To enable or disable Data Leak Prevention:

1. In the Administration Console tree, select the DLP Module settings node.
2. In the Data Leaks Prevention section, do one of the following:
   - Do disable Data Leak Prevention, clear the Enable Data Leak Prevention check box.
   - Do enable Data Leak Prevention, select the Enable Data Leak Prevention check box.
3. Click the Save button.

When Data Leak Prevention is enabled or disabled, the application performs the following operations:

- Sends the following notification to the addresses of security officers:
  - The administrator has disabled the DLP Module on all servers of the organization – when Data Leak Prevention is disabled;
  - The administrator has enabled the DLP Module on all servers of the organization – when Data Leak Prevention is enabled.

For a notification to be sent successfully, the notification delivery settings (see section “Configuring notification delivery settings” on page 103) must be configured in advance on the DLP query controller server (see section “Assigning the DLP query controller server” on page 100) or in the profile (see section “About profiles” on page 58) that includes the DLP query controller server. Otherwise, notifications will not be sent. Notifications can be received by security officers only if their addresses have been configured before notifications are sent (see the Security Officer’s Guide to Kaspersky Security 9.0 for Microsoft Exchange Servers).

If notification delivery has failed, an Error event with error information is recorded in the Windows application log on the DLP query controller server (see section “Assigning the DLP query controller server” on page 100).

- On each Security Server where Data Leak Prevention was disabled or enabled, the application adds the following event to the Windows Event Log:
  - “Level=Warning; Source=KSCM8; Event ID=16011” – when Data Leak Prevention is disabled;
  - “Level=Warning; Source=KSCM8; Event ID=16011” – when Data Leak Prevention is enabled;

After Data Leak Prevention is disabled, the application stops applying DLP policies to messages and scanning messages for data leaks. In this case, DLP databases are updated as usual.

ASSIGNING THE DLP QUERY CONTROLLER SERVER

By default, the DLP query controller server is the first corporate Security Server on which the DLP Module was installed first during application installation or upgrade. You can assign another Security Server on which the DLP Module is installed as a DLP query controller server.
To designate a DLP query controller server:

1. In the Administration Console tree, select the **DLP Module settings** node.
2. In the **DLP query controller server**, open a drop-down list and select the **Server name** of the Security Server that you want to assign as a DLP query controller server.
   
   This list shows only Security Servers on which the DLP Module is deployed.

3. Click the **Save** button.

**Configuring the connection to the DLP database**

By default, the DLP database is deployed along with the database of Backup and statistics. You can export tables from the DLP database to another database under a different name or deploy the DLP database on a different SQL server. You can also switch the application to use another instance of the DLP database that has been created in advance in case of a failure in the DLP database’s operation (e.g., due to an error on the SQL server). To do this, you need to configure the connection to the DLP database.

To configure the connection to the DLP database:

1. In the Administration Console tree, select the **DLP Module settings** node.
2. In the **DLP database configuration** section, configure the following settings:
   - **SQL server address and instance**. SQL server address in the following format: `<SQL server name>\<instance>`. The SQL server can be deployed on one of the Security Servers or on a dedicated computer on the corporate LAN.
   - **Database name**. The name of the DLP database that exists on the specified SQL server or a new DLP database.
   - **Redundant partner server**. Redundant partner server address in the following format: `<SQL server name>\<instance>`. Applies only to a fault-tolerant configuration of the SQL server with database mirroring (Failover). Optional field.
3. Click **Save** to save the changes.
   
   A confirmation window opens with a description of the actions that the application plans to implement.
4. Click **Yes** in the confirmation window.

   If the specified database exists, the application connects to it. Upon establishing a connection, the application checks the structure of the database and, if necessary, creates the missing tables. The structure of existing tables is not checked.

   If the specified database is missing, the application creates a new database with the specified name.

   To be able to successfully create a database and missing tables, your account must have the required permissions on the specified SQL server, presented in the table of privileges (see section “Step 5. Setting up the application's connection to the database of Backup and statistics” on page 26).

After successfully saving the changes made, the application starts using the database with the specified parameters as a DLP database. The application starts saving information about incidents, categories, and policies in this database.

When switching to a new DLP database, consider the following specifics:

- Incidents generated in the old DLP database remain in this database. Incidents are not copied to the new DLP database.
- Categories are not copied from the old DLP database to the new one. If the configured categories are missing in the new DLP database, any policies created on the basis of such categories are deleted.
- It takes 15 minutes to migrate to the new DLP database. During this time, some of the incidents that are generated may be saved in the old DLP database.

If your account does not have the permissions required to create the database and tables, the new DLP database can be created in advance by an employee with appropriate permissions, such as the database administrator. You can retrieve a ready script for creating the DLP database from the application and make it available to the relevant staff member to execute it.

To get the DLP database creation script,

- click the **Get DLP database creation script** link.

  The script opens in the window of the Notepad text editor.
NOTIFICATIONS

This section covers notifications and ways to configure them.

In this section:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About notifications</td>
<td>102</td>
</tr>
<tr>
<td>Configuring notification settings</td>
<td>102</td>
</tr>
<tr>
<td>Configuring notification delivery settings</td>
<td>103</td>
</tr>
</tbody>
</table>

ABOUT NOTIFICATIONS

Kaspersky Security can send notifications about infected, password-protected, and corrupted objects discovered while scanning. You can configure the application to send notifications about the revealed infected, protected and corrupted objects to the e-mail addresses of message sender, recipients, administrator and to additional addresses, for example, to security officers.

Notifications can be delivered using the following methods:

- By sending email messages. In this case you need to configure notification delivery settings (see section "Configuring notification delivery settings" on page 103).
- By registering the event in the Microsoft Windows system log on the computer where the Security Server is deployed. In this case, the information is accessible using Events viewer – a standard Microsoft Windows log viewing and management tool.

CONFIGURING NOTIFICATION SETTINGS

To define the notification settings, perform the following steps:

1. Perform the following steps in the Administration Console tree:
   - To configure notification settings for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To configure notification settings for Security Servers belonging to a profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to configure notification settings.

2. Select the Notifications node.

3. In the workspace, expand the relevant section to configure notifications of each type:
   - Notify about infected objects.
   - Notify about corrupted objects.
   - Notify about protected objects.
   - Notify about system events.

The application does not send system event notifications to the sender and the recipient.

4. Specify notification recipients in the Notify by email section for each type of notification.
   - If you want the application to send notifications to the administrator's email address, select the Administrator check box.
   - If you want the application to send notifications to the sender of the message in which the object has been detected, select the Sender check box.

The sender cannot be specified in the Notify about system events section.
If you want the application to send notifications to the recipient of the message in which the object has been detected, select the **Recipient** check box.

The recipient cannot be specified in the **Notify about system events** section.

If you want the application to send notifications to the specified email addresses, select **The following recipients** check box. In the entry field, specify the email address(es) to which the notifications should be sent.

5. When configuring system error notification settings, you can select events about which you want the application to send notifications in the **Notify about system events** configuration section. To this end, select the relevant check boxes:
   - **Notify about outdated databases.**
   - **Notify about events related to the license.**

6. If you want the application to record the event in the Microsoft Windows system log, select the **Register in Windows Event Log** check box.

7. Click the **Save** button.

If the application is running in a DAG of Microsoft Exchange servers, the notification settings configured on one of the servers will be automatically applied to all servers within the DAG. Configuring notifications on other servers of the DAG is not necessary.

### Configuring notification delivery settings

To define the notification sending settings, perform the following steps:

1. Perform the following steps in the Administration Console tree:
   - To configure notification delivery settings for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To configure notification delivery settings for Security Servers belonging to a profile, maximize the **Profiles** node and inside it maximize the node of the profile for whose Security Servers you want to configure notification delivery settings.

2. Select the **Notifications** node or the **Settings** node.

3. Depending on the node selected, do the following:
   - If you have selected the **Notifications** node, click the **Notification delivery settings** link in the lower part of the workspace to open the **Notification delivery settings** window.
   - If you have selected the **Settings** node, maximize the **Notification delivery settings** section.

4. In the **Exchange web service address** field, specify the address of the web service for sending notifications via the Microsoft Exchange server. The following address is used on the Microsoft Exchange server by default: `https://<name_of_client_access_server>/ews/exchange.asmx`

5. In the **Account** field, manually enter any account from mailboxes registered on the Microsoft Exchange server, or click the ... button and select an account in the window that opens.

6. Type the password for the selected account in the **Password** field.

7. In the **Administrator address** field, specify the mail recipient's address.

8. When configuring notification settings for an unassigned Security Server, you can send a test message by clicking the **Test** button.

   Test messages for Security Servers belonging to a profile are not supported.

9. Click **OK**.

If the application is running on a Microsoft Exchange DAG, the notification settings configured on one of the servers will be automatically applied to all servers within the DAG. Configuring delivery of notifications on other servers of the DAG is not necessary.
REPORTS

This section covers application reports and ways to configure them.

IN THIS SECTION:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About application reports</td>
<td>104</td>
</tr>
<tr>
<td>Generating a quick report</td>
<td>104</td>
</tr>
<tr>
<td>Creating a report generation task</td>
<td>105</td>
</tr>
<tr>
<td>Viewing the list of report generation tasks</td>
<td>106</td>
</tr>
<tr>
<td>Editing the settings of a report generation task</td>
<td>107</td>
</tr>
<tr>
<td>Starting a report generation task</td>
<td>107</td>
</tr>
<tr>
<td>Deleting a report creation task</td>
<td>107</td>
</tr>
<tr>
<td>Viewing Ready reports</td>
<td>108</td>
</tr>
<tr>
<td>Saving a report</td>
<td>109</td>
</tr>
<tr>
<td>Deleting a report</td>
<td>110</td>
</tr>
</tbody>
</table>

ABOUT APPLICATION REPORTS

Kaspersky Security supports creation and viewing of reports on the activity of the Anti-Virus and Anti-Spam modules. The application can generate a separate activity report for each module covering a period of one day or longer.

You can use the following report generation methods:

- Generate quick reports manually (see the section "Generating a quick report" on page 104).
- Generate reports using report generation tasks (see section "Creating a report generation task" on page 105). Report generation tasks can be started manually or automatically according to schedule. You can create new report generation tasks, delete or modify the existing ones.

The application supports standard and detailed reports. Standard reports contain information about objects that have been processed during the entire time period, without indication of the time when each individual event had occurred. Detailed reports specify the exact time spans in which the events occurred.

Time spans depend on the length of the reporting period selected:

- If the period is one day, the minimum time span for each event is one hour.
- If the period is two to seven days, the minimum time span for each event is six hours.
- If the period is eight or more days, the minimum time span for each event is 24 hours.

You can view the reports in the application or receive them via e-mail. E-mailed reports are appended to a message as an attachment. The message contains the following explanatory text: Attached file contains an activity report on Kaspersky Security 9.0 for Microsoft Exchange Servers.

CREATING QUICK REPORTS

To create a quick report, perform the following steps:

1. Perform the following steps in the Administration Console tree:
   - to create a report for an unassigned Security Server, maximize the node of the relevant Security Server;
   - to create a report for Security Servers belonging to one profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to generate a report.

2. Select the Reports node.
3. In the workspace, in the **View and create reports** section, click the **Create report** button.

4. In the **Quick report generation settings** window that opens, select one of the following items in the **Report type** drop-down list:
   - **Anti-Virus for the Mailbox role**, if you want to generate an Anti-Virus activity report for the Mailbox role.
   - **Anti-Virus for the Hub Transport role**, if you want to generate an Anti-Virus activity report for the Hub Transport role.
   - **Anti-Spam**, if you want to generate an Anti-Spam activity report.

5. Select one of the following items in the **Detail level** drop-down list:
   - To generate a report containing information about objects processed during the entire reporting period without indicating the time span during which a specific event occurred, select **Standard**.
   - To generate a detailed report indicating the time span during which a specific event occurred, select **Detailed**.
     The length of time spans depends on the length of the reporting period selected.

6. In the **from** and **to** fields, type the start and end dates of the period covered by the report or select them in the calendar.

7. To generate a report for Security Servers belonging to one profile, perform the following operations in the **Generate report based on statistics** sections:
   - Choose the **All profile servers** option to generate a report containing information about all Security Servers belonging to the profile. In the drop-down list on the right, select the Security Server where the report will be generated.
   - Choose the **Single server** option to generate a report containing information about a single Security Server in the profile. In the drop-down list on the right, select the Security Server for which you want to generate the report.

8. To create a quick report using the defined settings, click the **OK** button.

   The application opens the report window in a browser as soon as report generation has been completed and shows the report details in the **View and create reports** section.

**CREATING A REPORT GENERATION TASK**

*To create a report generation task:*

1. Perform the following steps in the Administration Console tree:
   - to create a report generation task for an unassigned Security Server, maximize the node of the relevant Security Server;
   - to create a report generation task for Security Servers belonging to one profile, maximize the **Profiles** node and inside it maximize the node of the profile for whose Security Servers you want to create the report generation task.

2. Select the **Reports** node.

3. In the workspace, in the **Report generation tasks** section, click the **New task** button.

4. In the **Scheduled report generation task** window that opens, enter the name of the task being created in the **Name** field.

5. One the **Report generation settings** tab, select one of the following items in the **Report type** drop-down list:
   - **Anti-Virus for the Mailbox role**, if you want to generate an Anti-Virus activity report for the Mailbox role.
   - **Anti-Virus for the Hub Transport role**, if you want to generate an Anti-Virus activity report for the Hub Transport role.
   - **Anti-Spam**, if you want to generate an Anti-Spam activity report.

6. Select one of the following report detail levels in the **Detail level** drop-down list:
   - To generate a report containing information about objects processed during the entire reporting period without indicating the time span during which a specific event occurred, select the **Standard** level of detail.
To generate a detailed report indicating the time span during which a specific event occurred, select the **Detailed** level of detail.

7. If you want the application to email the generated reports to the administrator's email address, select the **Send to the Administrator** check box.

8. If you want the application to send the generated reports to the specified email addresses, select **Send to recipients** check box. In the entry field, specify the email addresses to which the reports should be sent.

9. To generate a report for Security Servers belonging to one profile, perform the following operations in the **Generate report based on statistics** sections:
   - Choose the **All profile servers** option to generate reports containing information about all Security Servers belonging to the profile. In the drop-down list on the right, select the Security Server where the report will be generated.
   - Choose the **Single server** option to generate reports containing information about a single Security Server in the profile. In the drop-down list on the right, select the Security Server for which you want to generate the reports.

10. Select the **Generate scheduled report** check box on the **Schedule** tab if you want the application to generate reports in accordance with the specified schedule.

11. If you have selected the **Generate scheduled report** check box, specify the report generation frequency:
   - **Every N days.** In the **Every N days** entry field, specify the frequency of report generation in days. In the **Start time** entry field, specify the time when report generation should start.
   - **Weekly.** In the **Start day** section, select the days of the week on which the application should generate reports. In the **Start time** entry field, specify the time when report generation should start.
   - **Monthly.** In the **Day of the month** entry field, specify the day of the month on which the application should generate reports. In the **Start time** entry field, specify the time when report generation should start.

12. Click **OK**.

The application displays the created report generation task in the **Report generation tasks** section.

---

**VIEWING THE LIST OF REPORT GENERATION TASKS**

To view the list of report generation tasks:

1. Perform the following steps in the Administration Console tree:
   - to view report generation tasks for an unassigned Security Server, maximize the node of the relevant Security Server;
   - to view report generation tasks for Security Servers belonging to a profile, expand the **Profiles** node and, in this node, expand the node of the profile for whose Security Servers you want to view the report generation tasks.

2. Select the **Reports** node.

3. All tasks that have been created are displayed in the workspace, in the **Report generation tasks** section. The following information is displayed for each task:
   - **Task name** Name of the created report generation task.
   - **Type.** Generated report type: Anti-Spam, Anti-Virus for the Mailbox role or Anti-Virus for the Hub Transport role.
   - **Detail level.** Level of detail of the generated reports: detailed or standard.
   - **Scope.** A profile or a server covered by the reports being generated.
   - **Schedule.** The specified report generation schedule.
   - **Time of last modification.** The time when the report generation task was last modified.
   - **Next start.** The next start of the scheduled report generation task.
   - **Automatic start.** Indicates whether or not a task has been configured to start according to schedule.
   - **Generation server.** The server hosting the reports.
EDITING THE SETTINGS OF A REPORT GENERATION TASK

To edit the settings of a report generation task:

1. Perform the following steps in the Administration Console tree:
   - to edit the settings of a report generation task for an unassigned Security Server, maximize the node of the relevant Security Server;
   - to edit the settings of the report generation task for Security Servers belonging to a profile, expand the Profiles node and, in this node, expand the node of the profile for whose Security Servers you want to edit the settings of the report generation task.

2. Select the Reports node.

3. In the workspace, in the Report generation tasks section, select the task of which you want to edit the settings.

4. Click the Change button above the table of tasks.

5. In the Scheduled report generation task window, edit the relevant settings (see section "Creating a report creation task" on page 105).

6. Click OK.

STARTING A REPORT GENERATION TASK

To start a report generation task:

1. Perform the following steps in the Administration Console tree:
   - to start a report generation task for an unassigned Security Server, maximize the node of the relevant Security Server;
   - to start a report generation task for Security Servers belonging to a profile, expand the Profiles node and, in this node, expand the node of the profile for whose Security Servers you want to start the report generation task.

2. Select the Reports node.

3. In the workspace, in the Report generation tasks section, select the task that you want to run.

4. Click the Start task button.

The application opens the report window in a browser as soon as report generation has been completed and shows the report details in the View and create reports section.

DELETING A REPORT CREATION TASK

To delete a report generation task:

1. Perform the following steps in the Administration Console tree:
   - to delete a report generation task for an unassigned Security Server, maximize the node of the relevant Security Server;
   - to delete a report generation task for Security Servers belonging to a profile, expand the Profiles node and, in this node, expand the node of the profile for whose Security Servers you want to delete the report generation task.

2. Select the Reports node.

3. In the workspace, in the Report generation tasks section, select the task that you want to delete.

4. Click the Delete button above the table of tasks.

   A confirmation window opens.

5. Click Yes in the confirmation window.

   The selected task is deleted from the table of tasks in the Report generation tasks section.
VIEW THE READY REPORTS

To view the reports on Anti-Virus and Anti-Spam activity:

1. Perform the following steps in the Administration Console tree:
   - to view a report for an unassigned Security Server, maximize the node of the relevant Security Server;
   - to view a report for Security Servers belonging to a profile, expand the Profiles node and, in this node, expand the node of the profile for whose Security Servers you want to view the report.

2. Select the Reports node.

3. All reports that have been created are displayed in the workspace, in the View and create reports section. The table displays the following information about each report:
   - **Name.** The default name of the report.
   - **Created.** Report generation date and time.
   - **Interval.** The period of time covered by the report.
   - **Data source.** Name of the server, profile, DAG of servers (only for the Anti-Virus for the Mailbox role) covered in the report.
   - **Type.** Report type: Anti-Spam, Anti-Virus for the Mailbox role or Anti-Virus for the Hub Transport role.
   - **Detail level.** Level of detail of the report: detailed or standard.
   - **Generation server.** The server hosting the report.

4. To view a report, select it in the list and click the View button.
   The selected report opens in the default web browser window.

Viewing an Anti-Virus report

The header of the Anti-Virus report contains the following information:

- Report type.
- Name of the server or DAG for which the report was created.
- Period covered by the report.
- Day, month, year, and time of report generation (local time of the computer on which the report was generated).

You can view the following information in the standard Anti-Virus report table:

- **Status.** Object status after Anti-Virus processing.
- **Objects.** The number of objects with the specified status.
- **Percentage.** The share of objects with the specified status compared to the total number of objects.
- **Size.** Size of objects (messages, their parts or attachments) in megabytes.

You can view the following information in the detailed Anti-Virus report table:

- **Time period.** Time frame of object detection.
- **Non-infected objects.** The number of uninfected objects.
- **Disinfected objects.** The number of successfully disinfected objects.
- **Non-disinfected objects:**
  - **Infected objects.** Number of objects infected with viruses or their modifications.
  - **Probably infected objects.** The number of objects which may contain an unknown virus.
  - **Protected objects.** The number of password-protected objects, for example, archives.
  - **Corrupted objects.** Number of objects that cannot be disinfected because they are corrupted.
- **Unprocessed objects:**
  - **License problem.** The number of objects that have not been scanned because of a Kaspersky Security license problem.
  - **Anti-Virus database error.** The number of objects which have not been scanned because of corrupted or missing Anti-Virus databases.
  - **Processing error.** Number of objects that returned errors during scanning.
  - **Total objects.** The total number of objects referred for scanning.

The **For the entire period** row shows the total number of objects in each column for the entire reporting period.

### Viewing an Anti-Spam report

The header of the standard Anti-Spam report contains the following information:

- Day, month, year, and time of report generation (local time of the computer on which the report was generated).
- Report type.
- Name of the server for which the report has been generated.
- Period covered by the report.
- Servers covered in the report (if the report has been generated for a profile or DAG).

You can view the following information in the standard Anti-Spam report table:

- **Status.** Message status after Anti-Spam processing.
- **Number of messages.** The number of messages with the specified status.
- **Percentage.** The share of messages with the specified status as a percentage of all messages.
- **Size.** Message size in megabytes.

You can view the following information in the detailed Anti-Spam report table:

- **Time period.** Time frame during which messages arrived for processing.
- **Clean.** Number of messages that contain no spam or phishing links, and their size in megabytes.
- **Trusted.** Number of messages from trusted senders, and their size in megabytes.
- **Spam.** Number of spam messages, and their size in megabytes.
- **Potential spam.** Number of probable spam messages, and their size in megabytes.
- **Mass mailing.** Number of mass mailing messages that are not spam, and their size in megabytes.
- **Formal notifications.** Number of e-mails containing mail delivery confirmations and other service messages, and their size in megabytes.
- **Blacklisted.** Number of messages from blacklisted senders, and their size in megabytes.
- **Phishing.** Number of messages that contain phishing links.
- **Not scanned.** Number of messages that have not been scanned by Anti-Spam, and their size in megabytes.

The **For the entire period** row shows the total number of messages in each column for the entire reporting period, and their size in megabytes.

### Saving a report

**To save reports on Anti-Virus and Anti-Spam activity:**

1. Perform the following steps in the Administration Console tree:
   - to save a report for an unassigned Security Server, maximize the node of the relevant Security Server;
   - to save a report for Security Servers belonging to a profile, expand the **Profiles** node and, in this node, expand the node of the profile for whose Security Servers you want to save the report.

2. Select the **Reports** node.
3. In the table of reports in the View and create reports section, select the report you want to save and click the Save button.

4. In the Save as window that opens, specify the folder to which you wish to save the report and, if necessary, enter or modify the report name.

5. Click the Save button.

**DELETING A REPORT**

*To delete reports on Anti-Virus and Anti-Spam activity:*

1. Perform the following steps in the Administration Console tree:
   - to delete a report for an unassigned Security Server, maximize the node of the relevant Security Server;
   - to delete a report for Security Servers belonging to a profile, expand the Profiles node and, in this node, expand the node of the profile for whose Security Servers you want to delete the report.

2. Select the Reports node.

3. In the workspace, in the View and create reports section, select the report that you want to delete and click the Delete button.
   
   A confirmation window opens.

4. Click Yes in the confirmation window.

The selected report will be removed from the reports table.
APPLICATION LOGS

This section covers the application logs and ways to configure them.

IN THIS SECTION:

About application logs ................................................................. 111
Configuration of log settings ....................................................... 111
Configuring the detail level of logs .............................................. 112

ABOUT APPLICATION LOGS

Kaspersky Security records information about its operation (such as error messages or warnings) to Windows Event Log and to event logs of Kaspersky Security.

About Windows Event Log

Kaspersky Security records to Windows Event Log information that may be useful for Kaspersky Security administrators. This may include, e.g., error messages with hints to further actions.

Kaspersky Security events are marked in Windows Event Log with the acronym KSCM8 in the Source column.

About Kaspersky Security event logs


Kaspersky Security event logs are files in TXT format that are stored locally in the folder <Application installation folder>\logs. You can specify a different folder to store logs (see the section "Configuring logs" on page 111).

The detail of logs depends on the current settings of logs detail level (see the section "Configuring the detail level of logs" on page 112).

Kaspersky Security maintains event logs according to the following algorithm:

- The application records entries at the end of the most recent log.
- When the log’s size reaches 100 MB, the application archives it and creates a new one.
- The application stores log files for 14 days since the last modification, and then deletes them. You can set a different storage term for logs (see the section "Configuring logs" on page 111).

Separate logs are created individually for each Security Server irrespectively of the application deployment variant.

The folder with logs and the folder with the application data (<Application installation folder>\data) may contain confidential data. The application does not ensure protection against unauthorized access to data in those folders. You should take your own steps to protect the data in those folders against unauthorized access.

CONFIGURING LOG SETTINGS

To define the application logging settings, perform the following steps:

1. Perform the following steps in the Administration Console tree:
   - To configure log settings for an unassigned Security Server, maximize the node of the relevant Security Server;
   - To configure log settings for Security Servers belonging to one profile, maximize the Profiles node and inside it maximize the node of the profile for whose Security Servers you want to configure log settings.

2. Select the Settings node.
3. Expand the **Diagnostics** block of settings and perform the following actions:
   
   **a.** In the **Logs folder** field, specify the path to the folder for storing logs. You can reset the path to its default value by clicking the **Default** link. By default, the path `<Application installation folder>\logs` is set.

   No system variables (such as `%TEMP%`) are allowed to use in this string.

   You are advised to avoid using network folders as the logs folder. They are not supported by the application.

   You can specify the path to the logs folder for each Security Server individually. This parameter cannot be defined for a profile.

   If you specify a different folder to store logs, the application starts creating log files in this new folder. Older log files remain in the previously selected logs folder at that. If the new logs folder does not exist, it will be created. If the new folder cannot be accessed (e.g., due to lack of rights), the application records logs to the default folder until access to the new one is granted. The application switches to the new logs folder within 30 minutes after access to that folder is granted.

   **b.** In the **Log storage term** spin box, specify the time period during which logs will be stored in the folder after being created. When this period expires, the application deletes all logs.

   The default value is 14 days.

   **c.** Set up the diagnostics level (see the section “Configuring the detail level of logs” on page 112). The detail level determines the detail of logging.

   **d.** Select the **Notify about occurring errors by e-mail** check box if you want the application to email error notifications to the administrator simultaneously with logging them (see section “Configuring notification settings” on page 102).

4. Click the **Save** button.

   The application starts recording events to logs in accordance with the settings defined.

   If the application is running on a Microsoft Exchange server included in a DAG, the settings of logs that have been defined on one of the Microsoft Exchange servers will be automatically applied to the rest of the Microsoft Exchange servers included in the same DAG. You do not have to define the logging settings on other Microsoft Exchange servers in the same DAG.

### Configuring the Detail Level of Logs

To configure the detail level of event logs:

1. Perform the following steps in the Administration Console tree:
   - To configure the detail level of logs for an unassigned Security Server, expand the node of the relevant Security Server
   - To configure the detail level of logs for Security Servers belonging to a profile, expand the **Profiles** node and inside it expand the node of the profile in which you want to configure the diagnostics level of logs on the Security Servers.

2. Select the **Profiles** node.

3. Expand the **Diagnostics** block of settings.

4. Click the **Settings** button in the **Log detail** block of settings.

   This opens the **Diagnostics settings** window.

5. Select the events about which you want to log detailed information.

6. Click the **OK** button to save the changes and close the window.

   If you have selected multiple events in the window, the detail level changes to **Custom**. The application will log main events in the application's operation, as well as detailed information for the events that you have specified.

   If you have selected all of the events in the window, the detail level will change to **Maximum**. The application will log detailed information about all events.
Detailed application logging may slow the application down. Confidential information from the contents of messages can be recorded to detailed logs.

7. If you want to reset the current detail level of a log, click the **Reset** button.

   The application will change the detail level to **Minimum**. Only main events in the application’s operation will be logged, such as the result of scanning objects, the result of downloading updates for databases, and the result of adding a key.

8. Click **Save** to save the changes.

   If the application is running on a Microsoft Exchange server included in a DAG, the detail level that has been set on one of the Microsoft Exchange servers will be automatically applied to the rest of the Microsoft Exchange servers included in the same DAG. You do not have to configure the detail level on other Microsoft Exchange servers in the same DAG.
MANAGING CONFIGURATION

This section explains how you can export the application configuration to file and import it from file. The configuration file is in XML format.

In special cases, the application's behavior can be changed by creating a settings file of a dedicated format and moving that file to the application installation folder. For detailed information please refer to Technical Support.

IN THIS SECTION:

Exporting settings ................................................................. 114
Importing settings ................................................................. 115

EXPORTING SETTINGS

To export the application configuration to a file, perform the following steps:

1. In the Administration Console tree, expand the node of a Security Server.
2. Select the Settings node.
3. In the workspace, in the Configuration management section, click the Export button.
4. In the Select configuration parameters window that opens, select the check boxes for the groups of settings which you would like to export:
   - All settings. All settings that make up the configuration of the application.
   - Protection for the Hub Transport role. This group of settings applies to the Anti-Spam and Anti-Virus modules for the Hub Transport role.
   - Protection for the Mailbox role. This group of settings applies to the Anti-Virus component for the Mailbox role.
   - Advanced Anti-Virus settings. Advanced settings of Anti-Virus, such as KSN settings, scan settings for archives and containers, and exclusions from scanning.
   - Updates. Update settings of application databases.
   - Logging. The settings for application event logs and diagnostics.
   - Reports. Reporting settings.
   - Notifications. Notification settings
   - Infrastructure. This group includes the following settings:
     - Settings of the connection to the Microsoft SQL Server: server name and database name.
     - Proxy server settings.
5. Click OK.
6. In the Save as window that opens, enter the file name, select the destination folder, and click the Save button.

The application saves the selected configuration settings to a file with the .kseconfig extension.
**IMPORTING SETTINGS**

> To import the application settings from a file, perform the following steps:

1. In the Administration Console tree, expand the node of a Security Server.
2. Select the Settings node.
3. In the workspace, in the **Configuration management** section, click the **Import** button.
4. In the Open window that opens, select the file containing the application configuration and click the Open button.

Only files with the .kseconfig extension can be selected.

The application imports the configuration from the selected file. Parameter values loaded from the file will be used to replace current application settings without additional confirmations.
TESTING THE APPLICATION OPERATION

This section explains how to test the application in order to make sure that it detects viruses and their modifications and takes action on them.

IN THIS SECTION:

- About the EICAR test file .......................................................... 116
- About the types of the EICAR test file.......................................... 116
- Testing application performance using the EICAR test file........... 117

ABOUT THE EICAR TEST FILE

You can make sure that the application detects viruses and disinfects infected files by using a EICAR test file. The EICAR test file has been developed by the European Institute for Computer Antivirus Research (EICAR) in order to test the functionality of anti-virus applications.

The EICAR test file is not a virus. The EICAR test file does not contain any program code that could damage your computer. However, a major part of anti-virus applications identify the EICAR test file as a virus.

The EICAR test file is not intended for testing the functionality of the heuristic analyzer or searching for malware at the system level (rootkits).

Do not use real viruses to test the functionality of anti-virus applications! This may damage your computer.

Do not forget to resume the anti-virus protection of Internet traffic and files after you have finished with the EICAR test file.

ABOUT THE TYPES OF THE EICAR TEST FILE

You can test the application's functioning by creating various modifications of the EICAR test file. The application detects the EICAR test file (or a modification of it) and assigns it a status depending on the results of the scan. The application takes specified actions on the EICAR test file if they had been selected in the settings of the component that has detected the EICAR test file.

The first column of the table (see the table below) contains prefixes that you can use when creating modifications of the EICAR test file. The second column lists all possible statuses assigned to the file, based on the results of the scan by the application. The third column indicates how the application processes files with the specified status.

![Table 10. Modifications of the EICAR test file](image)

<table>
<thead>
<tr>
<th>PREFIX</th>
<th>FILE STATUS</th>
<th>FILE PROCESSING INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>No prefix, standard test virus.</td>
<td>Infected. File contains code of a known virus. File cannot be disinfected.</td>
<td>The application identifies this file as a file containing a virus that cannot be disinfected. The action set for infected files is applied to the file. By default, the application displays an on-screen notification that the file cannot be disinfected.</td>
</tr>
<tr>
<td>CURE-</td>
<td>Infected. File contains code of a known virus. File can be disinfected.</td>
<td>The file contains a virus that can be disinfected or deleted. The application disinfects the file; the text of the virus body is replaced with the word CURE. The application displays an on-screen notification that a disinfected file has been detected.</td>
</tr>
<tr>
<td>DELE-</td>
<td>Infected. File contains code of a known virus. File cannot be disinfected.</td>
<td>The application identifies the file as a virus that cannot be disinfected, and deletes it. The application displays an on-screen notification that the disinfected file has been deleted.</td>
</tr>
</tbody>
</table>
### TESTING THE APPLICATION OPERATION

<table>
<thead>
<tr>
<th>PREFIX</th>
<th>FILE STATUS</th>
<th>FILE PROCESSING INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>WARN-</td>
<td>Probably infected.</td>
<td>File is probably infected. The application applies the action set for potentially infected files on the file. By default, the application displays an on-screen notification that a potentially infected file has been detected.</td>
</tr>
<tr>
<td></td>
<td>File contains code of an unknown virus. File cannot be disinfected.</td>
<td></td>
</tr>
<tr>
<td>SUSP-</td>
<td>Probably infected.</td>
<td>The application detected a partial correspondence of a section of file code with a section of code of a known virus. When a potentially infected file is detected, the application databases do not contain a description of the full code of the virus. The application applies the action set for potentially infected files on the file. By default, the application displays an on-screen notification that a potentially infected file has been detected.</td>
</tr>
<tr>
<td></td>
<td>File contains modified code of a known virus. File cannot be disinfected.</td>
<td></td>
</tr>
<tr>
<td>CORR-</td>
<td>Corrupted.</td>
<td>The application does not scan this type of file because its structure is damaged (for example, the file format is invalid). You can find the information that the file has been processed in the report on the application's operation.</td>
</tr>
<tr>
<td>ERRO-</td>
<td>Scan error.</td>
<td>An error occurred during the scan of a file. The application could not access the file, since the integrity of the file has been breached (for example, no end to a multivolume archive) or there is no connection to it (if the file is scanned on a network drive). You can find the information that the file has been processed in the report on the application's operation.</td>
</tr>
</tbody>
</table>

### TESTING APPLICATION PERFORMANCE USING THE EICAR TEST FILE

After Kaspersky Security is installed and configured, you are advised to verify its settings and operation using the EICAR test file.

You can download the test file from the official EICAR website: [http://www.eicar.org/anti_virus_test_file.htm](http://www.eicar.org/anti_virus_test_file.htm).

You are strongly recommended to enable anti-virus protection of the server after you have finished using the EICAR test file. Disabling anti-virus protection of the server considerably increases the risk of malware infiltrating the e-mail system.

#### Testing the Anti-Virus functionality

- **To send a message with a test file:**
  1. Create an email message with the EICAR test file in the attachment.
  2. Send the message via a Microsoft Exchange server with Kaspersky Security installed and a Security Server connected (see the section "Adding Security Servers to Administration Console" on page 47).
  3. Check to make sure that the delivered message contains no virus.

When a virus is detected on a server deployed in the Mailbox role, the deleted virus is replaced with a text file. If a virus is detected on a server deployed in the Hub Transport role, the application adds the prefix Malicious object deleted to the message subject.

After virus detection, the mailbox that you have specified in the notification settings (see section "Configuring notifications" on page 102) receives a notification about the intercepted virus.

- **To view the application report on the detected virus:**
  1. In the tree of the Administration Console, expand the node of the Security Server through which the message with the EICAR test file in the attachment was sent.
  2. Select the **Reports** node.
3. In the workspace, in the **Quick reports** dropdown section, perform the following actions:
   a. In the **Type** drop-down list, select the type of report as **Anti-Virus for the Mailbox role** or **Anti-Virus for the Hub Transport role** (depending on the configuration).
   b. Click the **Create report** button.

4. View the generated report in the **View and create reports** drop-down settings section by selecting it in the list and clicking the **View** button.

If the report contains information about the EICAR infection, the application is properly configured.

**To configure the delivery of reports to the administrator's email address:**

1. In the tree of the Administration Console, expand the node of the Security Server through which the message with the EICAR test file in the attachment was sent.
2. Select the **Reports** node.
3. In the workspace, in the **Anti-Virus report for Mailbox role** and **Anti-Virus report for Hub Transport role** dropdown sections, in the **Send report to email address** section, select the **Administrator** check box to send notifications to the administrator's email address specified in the notification delivery settings (see the section "Configuring notification delivery settings" on page 103).
4. To make sure that reports arrive in the specified mailbox, click the **Test** button to send a test message.

By default, the application saves a copy of the infected object in Backup.

**To check whether a copy of an infected object has been saved in Backup, perform the following steps:**

1. In the tree of the Administration Console, expand the node of the Security Server through which the message with the EICAR test file in the attachment was sent.
2. Select the **Backup** node.
3. Make sure that the infected object (message with the EICAR test file in the attachment) appears in the table in the workspace.

**Testing the Anti-Spam functionality**

**To test the operation of Anti-Spam:**

1. In the tree of the Administration Console, expand the node of the Security Server through which the message with the EICAR test file in the attachment will be sent.
2. Select the **Server protection** node.
3. In the workspace, on the **Protection for Hub Transport role** tab, in the **Settings of Anti-Spam black and white lists** dropdown section, select the **Add sender's address to black list** check box.
4. In the entry field, type the email address of any mailbox to which you have access.
5. Click the **button on the right of the field.
6. On the **Protection for the Hub Transport role** tab, in the **Anti-Spam analysis settings** drop-down configuration list, open the **Spam processing settings** configuration section and for the **Blacklisted** status select the **Skip** item in the drop-down list and select the **Add label** check box.
7. Send a test message from the specified mailbox to the administrator's address through the protected mail server.

If the subject line of the incoming message contains the **[Blacklisted] label in the header**, Anti-Spam is working properly.
CONTACTING THE TECHNICAL SUPPORT SERVICE

This section describes the ways to get technical support and the terms on which it is available.

**In this section:**

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About technical support</td>
<td>119</td>
</tr>
<tr>
<td>Technical support by phone</td>
<td>119</td>
</tr>
<tr>
<td>Technical Support via Kaspersky CompanyAccount</td>
<td>119</td>
</tr>
<tr>
<td>Using a trace file and AVZ script</td>
<td>120</td>
</tr>
</tbody>
</table>

**About technical support**

If you could not find a solution to your problem in the documentation or in one of the sources of information about the application (see the section "Sources of information about the application" on page 10), we recommend that you contact Kaspersky Lab Technical Support. Technical Support specialists will answer your questions about installing and using the application.

Technical support is only available to users who purchased the commercial license. Users who have received a trial license are not entitled to technical support.

Before contacting Technical Support, we recommend that you read through the support rules [http://support.kaspersky.com/support/rules](http://support.kaspersky.com/support/rules).

You can contact Technical Support in one of the following ways:

- By calling Kaspersky Lab Technical Support.
- By sending a request to Technical Support through the Kaspersky CompanyAccount web service.

**Technical support by phone**

If an urgent issue arises, you can call Kaspersky Lab Technical Support representatives [http://support.kaspersky.com/support/contacts](http://support.kaspersky.com/support/contacts).

Before contacting Technical Support, you are advised to read the technical support rules [http://support.kaspersky.com/support/rules](http://support.kaspersky.com/support/rules). These rules contain information about the working hours of Kaspersky Lab Technical Support and about the information that you must provide so that Kaspersky Lab Technical Support specialists can help you.

**Technical Support via Kaspersky CompanyAccount**

Kaspersky CompanyAccount ([https://companyaccount.kaspersky.com](https://companyaccount.kaspersky.com)) is a web service for companies that use Kaspersky Lab applications. The Kaspersky CompanyAccount web service is designed to facilitate interaction between users and Kaspersky Lab specialists via online requests. You can use Kaspersky CompanyAccount to track the status of your online requests and store a history of them as well.

You can register all of your organization's employees under a single account on Kaspersky CompanyAccount. A single account lets you centrally manage electronic requests from registered employees to Kaspersky Lab and also manage the privileges of these employees via Kaspersky CompanyAccount.
The Kaspersky CompanyAccount web service is available in the following languages:

- English
- Spanish
- Italian
- German
- Polish
- Portuguese
- Russian
- French
- Japanese

To learn more about Kaspersky CompanyAccount, visit the Technical Support website (http://support.kaspersky.com/faq/companyaccount_help).

**USING A TRACE FILE AND AVZ SCRIPT**

After you report a problem to Kaspersky Lab Technical Support specialists, they may ask you to generate a report with information about the operation of Kaspersky Security and send it to Kaspersky Lab Technical Support. Kaspersky Lab Technical Support specialists may also ask you to create a *trace file*. A trace file helps track down step-by-step execution of application commands and detect the phase of application operation when an error occurs.

After analyzing the data you send, Kaspersky Lab Technical Support specialists can create an AVZ script and send it to you. By running AVZ scripts, it is possible to analyze active processes for threats, scan the computer for threats, disinfect or delete infected files, and create system scan reports.
APPENDIX. SCRIPT FOR SENDING SPAM FOR ANALYSIS

This section describes a script for sending spam for analysis to Kaspersky Lab specialists and how to configure it.

In this section:

- About the script for sending spam for analysis .......................................................... 121
- Script operation modes .................................................................................................. 121
- Script execution parameters .......................................................................................... 122
- Configuring parameters of the script configuration file ............................................... 123
- Script operation log ........................................................................................................ 124

About the script for sending spam for analysis

The Anti-Spam modules block spam messages using the currently known signatures of spam mailings. On receiving spam messages unknown to the Anti-Spam module, the user can send these unfiltered spam samples to Kaspersky Lab specialists for processing. This makes it possible to quickly add new signatures to the databases of the Anti-Spam module, block the spam mailing, thereby preventing any further deliveries of spam.

Users can send spam samples to Kaspersky Lab by placing them into the Junk Email folder. Spam messages can be located in the Junk Email folder of the mailboxes of specified users and sent to a specified address by means of a script for sending spam for analysis. The script sends only messages that were added to the Junk Email folder no sooner than the specified number of days back, provided that such messages have not been detected by other anti-spam mail protection systems.

The script sends messages from the Junk Email folder with their entire contents to Kaspersky Lab. You should warn users of mailboxes that moving messages to the Junk Email folder means confirming that those messages contain no confidential information.

The script is executed under an account that has an email address within the organization's Microsoft Exchange infrastructure and has access to Exchange Web Services. This account should have rights to edit the Junk Email folders in all mailboxes that are processed.

For purposes of keeping the log operation script and managing the configuration file with script settings, the account under which the script is executed should have privileges to write to the folder where the script is stored (<Application setup folder>SpamForwarder>).

To open the folder with the script,

```
select Start -> Programs -> Kaspersky Security 9.0 for Microsoft Exchange Servers -> Script for sending spam to research.
```

The program interface Microsoft Exchange Web Services Managed API 2.0 is required to run the script. Download the software module of this interface by clicking the following link: http://www.microsoft.com/en-us/download/details.aspx?id=35371 and store it in the bin subfolder of the folder containing the script.

Script operation modes

The script works in one of the two modes:

- Permission assignment mode
- Ordinary mode
Permission assignment mode

In the permission assignment mode, the script assigns mailbox access permissions to the user under whose account the script will be executed subsequently. You have to execute the script in this mode before you use it for the first time, as well as every time after adding new mailboxes to the configuration file.

Mailboxes for which rights have been assigned are marked with a special attribute in the configuration file. They are not processed by the script any time it runs in this mode.

You can reset privileges assigned by the script manually.

To reset permissions assigned by the script manually:
1. Open the user's mailbox in Microsoft Outlook®.
2. Open the context menu of the Junk Email folder.
4. On the Permissions tab of the properties window of the Junk Email folder, delete the entry linked to the user account under which the script is running.
5. Click OK.
6. Open the configuration file of the script (see section "Configuring parameters of the script configuration file" on page 123).
7. In the <users> section, delete the entry linked to the user's mailbox.

If you plan to stop processing spam messages from this mailbox, simply remove the rightsAssigned attribute from the entry in the configuration file. This will exclude the mailbox from processing until the script is executed in permission assignment mode again or until the rightsAssigned attribute is reset.

In permission assignment mode, the script is executed in Exchange Management Shell on behalf of the user with privileges to edit permissions in mailboxes of users.

The script requires Windows PowerShell™ version 2.0 or later.

Ordinary script operation mode

In this mode, the script selects spam messages one at a time from the Junk Email folder of users' mailboxes specified in the <users> section of the configuration file and for which the relevant rights have been assigned.

The following selection criteria are used:

- The message is not a non-delivery report (NDR)
- The message is not older than the number of days specified using the <oldMessages> parameter of the configuration file
- The "Subject" field of the message does not contain labels specified in the <subjectMarks> section of the configuration file

Every such spam message added to the email as an attachment, with the internal structure of the spam message retained, and sent to the email address specified using the <recipientEmail> parameter of the configuration file. After that, the label with the default attribute in the configuration file is added to the "Subject" field of the message.

This process is repeated for all mailboxes specified in the <users> section of the configuration file.

For the script to be executed continuously, use the tools of your operating system to create a scheduled task.

SCRIPT EXECUTION PARAMETERS

Regardless of the script mode, the script must be run with the -IWantToForwardEmailFromJunkEmailFolderToKasperskyLab parameter. This setting switches the script to active mode. When you attempt to run the script without this parameter, the script cannot run and the text of the program exception is displayed in Windows PowerShell console.
You can specify the following parameters as the input parameters for executing the script:

- **workFolder** – path to the folder where the script is located. By default, it is the path to the current folder. This parameter makes it possible to execute the script in normal mode.

**Example of the script executed in normal mode:**

```
..\spamForwarder.ps1 -workFolder c:\temp\spamForwarder -IWantToForwardEmailFromJunkEmailFolderToKasperskyLab
```

- **grantPermissions** – this parameter makes it possible to execute the script in permission assignment mode.

**Example of script execution in permission assignment mode:**

```
..\spamForwarder.ps1 -grantPermissions -IWantToForwardEmailFromJunkEmailFolderToKasperskyLab
```

## Configuring Parameters of the Script

**Configuration file**

The config.xml configuration file of the script makes it possible to configure the script execution parameters. It is structured as follows:

```xml
<config>
  <senderEmail>administrator@company.com</senderEmail>
  <recipientEmail>Probable_KSEspam@spam.kaspersky.com</recipientEmail>
  <exchangeVersion>Exchange2010</exchangeVersion>
  <envelopeSubject>Example of SPAM Message</envelopeSubject>
  <envelopeBody>This message contains SPAM sample in attachment</envelopeBody>
  <logSize>10</logSize>
  <oldMessages>3</oldMessages>
  <ews>https://kseserver.company.com/EWS/Exchange.asmx</ews>
  <users>
    <user rightsAssigned="True">user@company.com</user>
    <user>user1@company.com</user>
    <user>user2@company.com</user>
  </users>
  <subjectMarks>
    <mark>[KL SPAM]</mark>
    <mark default="True">[!! SPAM]</mark>
    <mark>[!!SPAM]</mark>
    <mark>[!!Spam]</mark>
    <mark>[!!Probable Spam]</mark>
    <mark>[!!Blacklisted]</mark>
  </subjectMarks>
</config>
```

You can redefine the following parameters of the script’s configuration file:

- **senderEmail** – the email address from which messages with spam samples are sent to Kaspersky Lab for analysis.

  The account under which the script is executed should have full privileges to manage the mailbox from which messages are sent to Kaspersky Lab.

- **recipientEmail** – email address to which spam samples are sent. The default address is Probable_KSEspam@spam.kaspersky.com.
- **exchangeVersion** – a parameter describing the Microsoft Exchange version for initializing EWS API; it can take one of the following values (you have to choose the most appropriate value):
  - Exchange2010;
  - Exchange2010_SP1;
  - Exchange2013.
- **envelopeSubject** – the subject of the message to which spam samples are attached before it is sent. Changing this value is not recommended.
- **envelopeBody** – the body of the message to which spam samples are attached before it is sent. Changing this value is not recommended.
- **logSize** – the maximum size of the log file (megabytes) upon which rotation is performed. You can specify any value.
- **oldMessages** – the maximum age of messages (in days) that the script selects for transmission. The default value is 3 days. Changing this value is not recommended.
- **ews** – address of the EWS service. If this parameter is present in the configuration file, the script does not use the option that automatically detects the CA of the server. Using this parameter is not recommended.
- **users** – a section containing the email addresses of users whose mailboxes are processed by the script. This section can contain a random number of entries with individual mailboxes of users.
- **user** – an entry containing the email address of the mailbox to be processed by the script. The **rightsAssigned** attribute is inserted automatically when the rights are assigned. Changing this value manually is not recommended, unless you need to reassign rights to a user's mailbox. Entries for which this attribute is not set are skipped by the script.
- **subjectMarks** – a section containing possible labels that are added by anti-spam systems to the message subject. This section can contain a random number of entries. However, the number of different labels can affect the speed of the search for messages in user mailboxes.
- **mark** – an entry containing an individual label. The **default** attribute marks the entry that is used by the script to label the messages sent for analysis. It is not recommended to set the **default** attribute for several labels, as doing so would disrupt the operation of the script.

**SCRIPT OPERATION LOG**

The results of the script's activity are saved to a log file. The script log is located in the folder that stores the script, in the *log* subfolder.

The current size of the log file is estimated every time the script is executed. If the size of the log file exceeds the value specified in the `<logSize>` parameter of the configuration file, the log is archived using the GZIP method. At this stage, a check is performed to detect any file log archives older than two months. Such archives are deleted.
GLOSSARY

A

ACTIVE KEY
Key that is used at the moment to work with the application.

ADDITIONAL KEY
Key that verifies the use of the application but is not used at the moment.

ADMINISTRATION CONSOLE
Kaspersky Security application component. Provides the user interface for managing the application’s administrative services and enables configuration of the application and management of the server component. The management module is implemented as an extension of the Microsoft Management Console (MMC).

ANTI-VIRUS DATABASES
Databases that contain information about computer security threats known to Kaspersky Lab as of the anti-virus database release date. Anti-virus database signatures help to detect malicious code in scanned objects. Anti-virus databases are created by Kaspersky Lab specialists and updated hourly.

B

BACKUP
Special storage for backup copies of objects saved before their disinfection, removal or replacement. It is a service subfolder in the application data folder created during Security Server installation.

BLACK LIST OF KEY FILES
Database that contains information about the key files blocked by Kaspersky Lab. The black list file content is updated along with the product databases.

C

CONTAINER OBJECT
An object consisting of several objects, for example, an archive or a message with an attached letter. See also simple object.

D

DNS BLOCK LIST (DNSBL)
Public lists of IP addresses known to generate spam.

DISINFECTION
A method of processing infected objects that results in full or partial recovery of data. Not all infected objects can be disinfected.

E

ENFORCED ANTI-SPAM UPDATES SERVICE
The service providing quick updates to the Anti-Spam database improving the efficiency of Anti-Spam against new emerging spam. To function properly, Enforced Anti-Spam Updates Service needs a permanent Internet connection.
F

FILE MASK
Representation of a file name using wildcards. The standard wildcards used in file masks are * and ?, where * represents any number of any characters and ? stands for any single character.

FORMAL MESSAGE
Notifications which are automatically generated and sent by mail programs or robots (for instance, informing about the inability to deliver a letter or confirming user registration on a web site).

I

INFECTED OBJECT
An object a portion of whose code completely matches part of the code of known malware. Kaspersky Lab does not recommend using such objects.

K

KASPERSKY LAB UPDATE SERVERS
HTTP and FTP servers of Kaspersky Lab from which Kaspersky Lab applications download database and application module updates.

KASPERSKY SECURITY NETWORK (KSN)
Infrastructure of online services providing access to the current knowledge base of Kaspersky Lab describing the reputation of files, web sites and software. The use of data from Kaspersky Security Network ensures faster response by Kaspersky Lab applications to unknown threats, improves the effectiveness of some protection components, and reduces the risk of false positives.

L

LICENSE TERM
A time period during which you have access to the application features and rights to use additional services. Available functionality and specific additional services depend on the license type.

M

MALICIOUS URLS
Web addresses leading to malicious resources, i.e. web resources designed to spread malware.

MESSAGE DELETION
Method of processing an e-mail message which entails physical removal of the message. It is recommended to apply this method to messages which unambiguously contain spam or malicious objects. Before deleting a message, a copy of it is saved in Backup (unless this option is disabled).

O

OBJECT REMOVAL
A method of processing objects that involves physically removing them from their original location. We recommend that this method be applied to dangerous objects which, for whatever reason, cannot be disinfected.
PCL rating
Phishing Confidence Level is a special tag used by Microsoft Exchange mail servers to measure the probability of the risk of phishing threats in a message. The PCL rating ranges from 0 to 8. A mail server considers a message with a PCL rating of 3 or lower to be free from phishing threats. A message with a rating of 4 or higher is considered a phishing message. Kaspersky Security can change the PCL rating of a message depending on the message scan results.

Phishing
A kind of online fraud aimed at obtaining unauthorized access to confidential data of users.

Potential spam
A message that cannot be unambiguously considered spam, but has several spam attributes (e.g., certain types of mailings and advertising messages).

Probably infected object
An object whose code contains a modified segment of code of a known threat, or an object resembling a threat in the way it behaves.

Profile
A set of settings applied simultaneously to several Security Servers.

Proxy server
A computer network service which allows users to make indirect requests to other network services. First, a user connects to a proxy server and requests a resource (e.g., a file) located on another server. Then the proxy server either connects to the specified server and obtains the resource from it or returns the resource from its own cache (if the proxy has its own cache). In some cases, a user’s request or a server’s response can be modified by the proxy server for certain purposes.

SCL rating
Spam Confidence Level is a special tag used by Microsoft Exchange mail servers to measure the spam probability of a message. The SCL rating can range from 0 (minimum probability of spam) to 9 (the message is most probably spam). Kaspersky Security can change the SCL rating of a message depending on the message scan results.

Security Server
Server component of Kaspersky Security. Scans e-mail traffic for viruses and spam, performs anti-virus database updates, ensures the integrity of the application and its data storage, and enables administrative services for remote management and configuration. The component includes one or several interceptors.

Simple object
Message body or simple attachment, for example, an executable file. See also container object.

Spam
Unsolicited mass e-mail, most often containing advertising messages.

Spam URI Realtime Block Lists (SURBL)
Public lists of hyperlinks to the resources advertised by spam senders.

Storage scan
Anti-virus scanning of messages stored on an e-mail server and the content of public folders using the latest database version. Background scans can be launched either automatically (using a schedule) or manually. The scan involves all protected public folders and mailbox storages. Scanning may reveal new viruses that had not been included in the database during earlier scans.
**U**

**Un**known **v**irus

A new virus that is not yet registered in the databases. The application usually detects unknown viruses in objects by means of the heuristic analyzer. Such objects are labeled as probably infected.

**Update**

A function performed by a Kaspersky Lab application that enables it to keep computer protection up-to-date. During the update, an application downloads updates for its databases and modules from Kaspersky Lab’s update servers and automatically installs and applies them.

**V**

**V**irus

A program that infects other ones by adding its code to them in order to gain control when infected files are run. This simple definition allows exposing the main action performed by any virus – infection.
KASPERSKY LAB ZAO

Kaspersky Lab software is internationally renowned for its protection against viruses, malware, spam, network and hacker attacks, and other threats.

In 2008, Kaspersky Lab was rated among the world’s top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab is the preferred developer of computer protection systems among home users in Russia, according to the COMCON survey “TGI-Russia 2009”.

Kaspersky Lab was founded in Russia in 1997. Today, it is an international group of companies headquartered in Moscow with five regional divisions that manage the company’s activity in Russia, Western and Eastern Europe, the Middle East, Africa, North and South America, Japan, China, and other countries in the Asia-Pacific region. The company employs more than 2000 qualified specialists.

PRODUCTS. Kaspersky Lab’s products provide protection for all systems—from home computers to large corporate networks.

The personal product range includes anti-virus applications for desktop, laptop, and tablet computers, and for smartphones and other mobile devices.

Kaspersky Lab delivers applications and services to protect workstations, file and web servers, mail gateways, and firewalls. Used in conjunction with Kaspersky Lab’s centralized management system, these solutions ensure effective automated protection for companies and organizations against computer threats. Kaspersky Lab’s products are certified by the major test laboratories, are compatible with the software of many suppliers of computer applications, and are optimized to run on many hardware platforms.

Kaspersky Lab’s virus analysts work around the clock. Every day they uncover hundreds of new computer threats, create tools to detect and disinfect them, and include them in the databases used by Kaspersky Lab applications. Kaspersky Lab’s Anti-Virus database is updated hourly, and the Anti-Spam database—every five minutes.

TECHNOLOGIES. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. This is one of the reasons why many third-party software developers have chosen to use the Kaspersky Anti-Virus engine in their own applications. Those companies include SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Openwave Messaging (Ireland), D-Link (Taiwan), M86 Security (USA), GFI Software (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), Netasq-Arkoon (France), NETGEAR (USA), Parallels (USA), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Many of the company’s innovative technologies are patented.

ACHIEVEMENTS. Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. For example, in 2010 Kaspersky Anti-Virus received several top Advanced+ awards in a test administered by AV-Comparatives, a respected Austrian anti-virus laboratory. But Kaspersky Lab’s main achievement is the loyalty of its users worldwide. The company’s products and technologies protect more than 300 million users, and its corporate clients number more than 200,000.

Kaspersky Lab’s website: http://www.kaspersky.com
Virus Encyclopedia: http://www.viruslist.com
Anti-Virus Lab: http://newvirus.kaspersky.com (for scanning suspicious files and websites)
Kaspersky Lab's web forum: http://forum.kaspersky.com
INFORMATION ABOUT THIRD-PARTY CODE

Information about third-party code is contained in a file named legal_notices.txt and stored in the application installation folder.
TRADEMARK NOTICE

Registered trademarks and service marks are the property of their respective owners.
Active Directory, Access, Microsoft, Outlook, SQL Server, Windows, Windows Server, Windows Vista and Windows PowerShell are trademarks of Microsoft Corporation registered in the USA and other countries.
Intel and Pentium are trademarks of Intel Corporation registered in the USA and other countries.
# INDEX

## A

- Actions on objects ................................................................. 74
- Actions on spam ................................................................. 84
- Adding a server ........................................................................ 47
- Administration Console starting .............................................. 15
- Anti-Phishing ........................................................................... 46
- Anti-Spam ............................................................................... 83
- Anti-virus protection ............................................................... 80
- Application architecture .......................................................... 69
- Application components .......................................................... 15
- Application Configuration Wizard ........................................... 28
- Application databases ............................................................. 34
- Application interface ............................................................... 35
- Application setup .................................................................... 36
- Attachments ............................................................................ 37
- AVZ script ............................................................................. 120

## B

- Background scan ..................................................................... 78
- Backup .................................................................................... 93
  - configuring settings .............................................................. 97
  - deleting an object ............................................................... 96
- Backup and statistics database ............................................... 97

## C

- Configuring notification settings ............................................ 30
- Console tree .......................................................................... 35
- Context menu ....................................................................... 36
- Custom installation ............................................................... 25
- Custom Installation ................................................................ 25

## D

- Databases automatic update .................................................. 65
  - manual update .................................................................. 66
  - scheduled update ............................................................ 65
- Deployment models ............................................................... 20
- Diagnostics .......................................................................... 112

## E

- EICAR .................................................................................... 116, 117
- Event log ............................................................................... 111
  - configuring settings .......................................................... 111
- Exclusions Activity filtering .................................................. 75

## G

- Getting started ...................................................................... 28

## H

- Hardware and software requirements .................................... 13
<table>
<thead>
<tr>
<th>Index</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial configuration</td>
<td>28</td>
</tr>
<tr>
<td>Installation types</td>
<td>25</td>
</tr>
<tr>
<td>K</td>
<td></td>
</tr>
<tr>
<td>Kaspersky Security Network</td>
<td>29, 72</td>
</tr>
<tr>
<td>Key</td>
<td>29, 39</td>
</tr>
<tr>
<td>L</td>
<td></td>
</tr>
<tr>
<td>License</td>
<td>37</td>
</tr>
<tr>
<td>End User License Agreement</td>
<td>37</td>
</tr>
<tr>
<td>key file</td>
<td>38</td>
</tr>
<tr>
<td>M</td>
<td></td>
</tr>
<tr>
<td>Main window</td>
<td>34</td>
</tr>
<tr>
<td>Console tree</td>
<td>34</td>
</tr>
<tr>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Notifications</td>
<td>102</td>
</tr>
<tr>
<td>P</td>
<td></td>
</tr>
<tr>
<td>Profile</td>
<td>58</td>
</tr>
<tr>
<td>Protection</td>
<td>72, 83</td>
</tr>
<tr>
<td>enabling / disabling</td>
<td>74</td>
</tr>
<tr>
<td>Protection for mailboxes</td>
<td>74</td>
</tr>
<tr>
<td>Protection of public folders</td>
<td>48</td>
</tr>
<tr>
<td>Protection status</td>
<td>30, 67</td>
</tr>
<tr>
<td>Proxy server</td>
<td></td>
</tr>
<tr>
<td>Removing the application</td>
<td>32</td>
</tr>
<tr>
<td>Report creation task</td>
<td>104</td>
</tr>
<tr>
<td>creating</td>
<td>104</td>
</tr>
<tr>
<td>Reports</td>
<td>105</td>
</tr>
<tr>
<td>creating</td>
<td>104</td>
</tr>
<tr>
<td>creation tasks</td>
<td>105</td>
</tr>
<tr>
<td>quick reports</td>
<td>104</td>
</tr>
<tr>
<td>saving</td>
<td>109</td>
</tr>
<tr>
<td>viewing</td>
<td>108</td>
</tr>
<tr>
<td>Restoring the application</td>
<td>32</td>
</tr>
<tr>
<td>S</td>
<td></td>
</tr>
<tr>
<td>Scan exclusions</td>
<td>75</td>
</tr>
<tr>
<td>Scanning messages</td>
<td>80, 83</td>
</tr>
<tr>
<td>Security Server</td>
<td>15</td>
</tr>
<tr>
<td>Selecting components to install</td>
<td>25</td>
</tr>
<tr>
<td>Server protection</td>
<td>29</td>
</tr>
<tr>
<td>Setup Wizard</td>
<td>24</td>
</tr>
<tr>
<td>Software requirements</td>
<td>13</td>
</tr>
<tr>
<td>Start</td>
<td></td>
</tr>
<tr>
<td>application</td>
<td>46</td>
</tr>
<tr>
<td>manual update</td>
<td>64</td>
</tr>
<tr>
<td>report creation</td>
<td>107</td>
</tr>
<tr>
<td>Starting</td>
<td>46</td>
</tr>
<tr>
<td>Administration Console</td>
<td></td>
</tr>
<tr>
<td>T</td>
<td></td>
</tr>
<tr>
<td>Testing performance</td>
<td>117</td>
</tr>
</tbody>
</table>
Toolbar .......................................................................................................................... 34
Tracing
   Trace file .................................................................................................................. 120
U
Update ............................................................................................................................. 63
   manual run ................................................................................................................. 64
   proxy server .............................................................................................................. 67
   scheduled update ...................................................................................................... 65
   update source .......................................................................................................... 66
Update source .................................................................................................................. 66
Upgrading the application ............................................................................................... 30