Kaspersky Security 9.0 for SharePoint Server

Administrator's Guide

Application version: 9.0 Maintenance Release 2

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 AO Kaspersky Lab (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 fhttp://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: 10/10/2015

http://www.kaspersky.com
https://help.kaspersky.com
http://support.kaspersky.com

Table of Contents

About this Guide

This document is the Administrator's Guide to Kaspersky Security 9.0 for SharePoint® Server.

The Administrator's Guide to Kaspersky Security 9.0 for SharePoint Server (hereinafter "Kaspersky Security") is intended for professionals who install and administer Kaspersky Security, as well as for those who provide technical support to organizations that use Kaspersky Security.

This Guide provides instructions on:

- Preparing Kaspersky Security for installation, installing and activating the application
- Configuring and using Kaspersky Security

This Guide also lists sources of information about the application and ways to get technical support.

In this section

In this document

This document includes the following sections:

Sources of information about the application (see page 13)

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 SharePoint Server (see page 16)

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 23)

This section describes the Kaspersky Security components and their interaction.

Role-based access restriction in Kaspersky Security for SharePoint Server (see page 26)

This section contains information on how to restrict access to Kaspersky Security features by means of roles.

Access rights for managing Kaspersky Security (see page 28)

This section contains information on the sets of privileges required to install and administer the application, start application services and manage the SQL database.

Installing and removing the application (see page 32)

This section provides instructions on how to install and remove the application, as well as information about system changes after installation of the application.

Application licensing (see page 55)

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.

Getting started (see page 68)

This section provides information about how to start using Kaspersky Security and how to add SharePoint servers with installed Security Server to Administration Console.

Protection status of servers (see page 70)

This section describes how to check the protection level of Security Servers using Administration Console, i.e., how to view the licensing details, the status of application modules, as well as the statistics on objects scanned and threats detected.

Default server protection (see page 78)

This section describes how Kaspersky Security operates with default settings.

On-access scanning (see page 79)

This section provides information about the protection of SharePoint servers in real-time mode, as well as instructions on how to configure the protection.

On-demand scanning (see page 92)

This section provides information about how to scan SharePoint servers in background mode, as well as instructions on how to configure scanning.

Scanning of SharePoint content (see page 105)

This section provides information about how to scan web objects for unwanted content, malicious or phishing URLs, as well as instructions on how to configure the scanning.

Configuring application settings (see page 115)

This section contains information about advanced application settings and how to configure them.

Updating databases (see page 74)

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

Sending automatic notifications (see page 128)

This section provides information about types of events in the application's operation, as well as instructions on how to configure the notification about those events.

Backup (see page 135)

This section contains information about Backup and how to use it.

Managing reports (see page 146)

This section provides information about types of reports in the application, as well as instructions on how to configure the creation of those reports.

Application logs (see page 155)

This section provides information about the logs of Kaspersky Security and how to define the settings for maintaining those logs.

Contacting Technical Support (see page 160)

This section describes the ways to get technical support and the terms on which it is available.

Glossary (see page 163)

This section contains a list of terms mentioned in the document and their respective definitions.

AO Kaspersky Lab (see page 168)

This section provides information about AO Kaspersky Lab.

Information about third-party code (see page 170)

This section provides information about third-party code used in the application.

Trademark notices (see page 171)

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

The following conventions are used herein (see table below).

Table 1. Document conventions

Sample text	Document conventions description
Note that...	Warnings are highlighted in red and enclosed in frames. Warnings contain information about actions that may lead to some unwanted results.
It is recommended that you use...	Notes are enclosed in frames. Notes contain additional and reference information.

Sample text	Document conventions description
Example:	Examples are given on a blue background under the heading "Example".
An *update* is... The *Databases are outdated* event occurs.	The following items are italicized: • new terms; • status variations and application events.
Press **ENTER**. Press **ALT**+**F4**.	Names of keyboard keys appear in bold and are capitalized. Names of keys linked with a + (plus) sign indicate key combinations. Such keys should be pressed simultaneously.
Click the **Enable** button.	UI elements, for example, names of entry fields, menu items, buttons are in bold.
► *To configure a task schedule, perform the following steps:*	Introductory phrases of instructions are printed in italics and marked with an arrow sign.
Enter `help` in the command line The following message will appear: `Specify the date in DD:MM:YY format.`	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 that should be entered at the keyboard.
<User name>	Variables are enclosed in angle brackets. Instead of a variable, the corresponding value should be inserted, with angle brackets omitted.

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

You can use the following sources to search for information about Kaspersky Security on your own:

- Kaspersky Security page on the Kaspersky Lab website
- Kaspersky Security 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.

> An Internet connection is required to use online information sources.

Kaspersky Security page on the Kaspersky Lab website

On the Kaspersky Security page (http://www.kaspersky.com/business-security/microsoft-sharepoint), you can view general information about the application, its functions and features.

The Kaspersky Security page contains a link to eStore. There you can purchase the application or renew your license.

Kaspersky Security page in the Knowledge Base

Knowledge Base is a section on the Technical Support website.

On the Kaspersky Security page in the Knowledge Base (http://support.kaspersky.com/ksh9), you can read articles that provide useful information, recommendations, and answers to frequently asked questions on how to purchase, install, and use the application.

Knowledge Base articles can answer questions relating to not only to Kaspersky Security but also to other Kaspersky Lab applications. Knowledge Base articles can also include Technical Support news.

Online help

The application includes full help and context help files.

Context help provides information about Kaspersky Security windows: descriptions of Kaspersky Security settings and links to descriptions of tasks that use such settings.

Full help provides information on how to configure and use Kaspersky Security.

Help files can be included in the application or published online on a Kaspersky Lab web resource. If help files are published online, they open in a web browser window when you try to access them. An Internet connection is required to view online help.

Documentation

Application documentation consists of the files of application guides.

- The Administrator's Guide provides instructions on:
- Preparing Kaspersky Security for installation, installing and activating the application
- Configuring and using Kaspersky Security

The Security Officer's Guide provides information about standard tasks that a user can perform through the application, with regard for rights granted in Kaspersky Security.

The Help Guide provides the descriptions of Kaspersky Security features and settings. The sections of the Help Guide are sorted in alphabetical order or grouped by topic.

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 SharePoint Server

Kaspersky Security is an application for protection of servers running Microsoft® SharePoint Server against malicious objects and unwanted content.

Kaspersky Security can perform the following operations:

- Scan on demand various documents stored on the SharePoint servers checking them for the presence of harmful objects and unwanted content.
- Perform on-access scan of documents placed on SharePoint servers. Kaspersky Security scans documents checking them for the presence of harmful objects or unwanted content when users attempt to upload a document to server or download it from server to a workstation.
- Scan on demand files attached to items within SharePoint lists checking them for the presence of unwanted content.
- Select areas of the SharePoint structure to scan on demand, and exclude certain areas from the scan to reduce the load on the server.
- Configure the rules for processing of the documents in which harmful objects or unwanted content are detected.
- Save copies of the documents in Backup before disinfecting or deleting them.
- Generate reports about the results of document scanning. Reports can be generated automatically in accordance with the defined schedule or upon request.

In this section

About Kaspersky Security 9.0 for SharePoint Server

Kaspersky Security 9.0 for SharePoint Server Maintenance Release 2 (hereinafter referred to as "the application") is designed to protect the SharePoint platform against viruses and other malware. The application lets you scan the content of websites and wiki blogs for unwanted content, protect personal data of users, and confidential corporate data on SharePoint websites against data leaks.

Kaspersky Security features:

- Scan files for malware and unwanted content in real time
- Block files containing malware or unwanted content at the attempt to upload them to SharePoint;
- Monitor the content of blogs and wiki pages on SharePoint
- Form custom criteria of unwanted content
- Scan web addresses against lists of malicious or phishing links
- Receive anti-virus database updates from Kaspersky Lab servers during the license validity period
- Use file and link reputation data from Kaspersky Security Network services
- Scan files on SharePoint in background mode
- Configure the schedule and run mode of SharePoint file scan tasks
- Move copies of infected objects to Backup before disinfecting or deleting them
- Automatically or manually generate application reports and send them to email addresses
- Define the settings for maintaining the application event logs
- Automatically send infected file notifications to email addresses
- Use the role-based access control system for accessing various application functions

- Create data categories to protect information that is valuable to the company;
- Scan file content for data of specific categories at the time when users upload files to SharePoint sites.

What's new

Kaspersky Security offers the following new features:

- Configuring text templates for notifications of application operation events (for the administrator)
- Changing the set of any Kaspersky Lab category (for the data security officer)
- Calling Help in online mode

The Management Console GUI has also been improved.

Distribution kit

Kaspersky Security 9.0 for SharePoint Server is supplied as part of the applications Kaspersky Security for collaboration servers (http://www.kaspersky.com/business-security/collaboration) and Kaspersky Total Security (http://www.kaspersky.com/business-security/total).

You can purchase the application through partner companies or at Kaspersky Lab eStore (http://www.kaspersky.com/store).

If the application is purchased through an online store, it is downloaded from the store's website. Information needed to active the application, including the key file, will be emailed to you after you purchase a license.

Files of online help and documentation for the application are included in the distribution kit downloaded from the eStore website. Documentation files can be downloaded separately from Kaspersky Lab website http://www.kaspersky.com/documentation/sharepoint.

Carefully review the End User License Agreement between installing and using the application.

Hardware and software requirements

Kaspersky Security has the following hardware and software requirements:

Hardware requirements

For SharePoint Server 2010:

- If installing Administration Console and Security Server:
  - 64-bit quad-core processor
  - 4 GB RAM
  - 229 MB of available disk space
- If installing only Administration Console:
  - Minimum 400 MHz processor (1 GHz recommended)
  - 256 MB RAM
  - 176 MB of available disk space

For SharePoint Server 2013, SharePoint Server 2016:

- If installing Administration Console and Security Server:
  - 64-bit quad-core processor
  - 8 GB RAM
  - 229 MB of available disk space
- If installing only Administration Console:
  - Minimum 400 MHz processor (1 GHz recommended)
  - 256 MB RAM
  - 176 MB of available disk space

Depending upon the application settings and its mode of operation, more disk space may be required for Backup and other service folders. DLP Module additionally requires at least 4 GB free disk space. While DLP Module is running, files and memory dumps are generated, which may require a volume of memory that would significantly exceed 4 GB.

Software requirements

Required components to install the application:

- Microsoft SharePoint 2010, Microsoft SharePoint 2013 or Microsoft SharePoint 2016

  Standalone installation of Administration Console does not require Microsoft SharePoint Server

- Microsoft .NET Framework 3.5 Service Pack 1
- Microsoft Management Console 3.0

Supported versions of SharePoint servers:

- Microsoft SharePoint 2010
- Microsoft SharePoint 2013
- Microsoft SharePoint 2016

Supported operating systems:

For SharePoint Server 2010:

- If installing Administration Console and Security Server:
  - Windows Server® 2008 R2 Service Pack 1
  - Windows Server 2012 R2
- If installing only Administration Console:
  - Windows Server 2008 R2
  - Windows Server 2012 x64

    - Windows Server 2012 R2
    - Windows® 7 Professional Service Pack 1
    - Windows 7 Professional x64 Service Pack 1
    - Windows 7 Enterprise Service Pack 1
    - Windows 7 Enterprise x64 Service Pack 1
    - Windows 7 Ultimate Service Pack 1
    - Windows 7 Ultimate x 64 Service Pack 1
    - Windows 8
    - Windows 8 x64
    - Windows 8.1
    - Windows 10

For SharePoint Server 2013, SharePoint Server 2016:

- If installing Administration Console and Security Server:
    - Windows Server 2008 R2 x64 Service Pack 2
    - Windows Server 2012 x64
    - Windows Server 2012 R2
- If installing only Administration Console:
    - Windows Server 2008 R2
    - Windows Server 2012 x64
    - Windows Server 2012 R2
    - Windows 7 Professional Service Pack 1
    - Windows 7 Professional x64 Service Pack 1

- Windows 7 Enterprise Service Pack 1
- Windows 7 Enterprise x64 Service Pack 1
- Windows 7 Ultimate Service Pack 1
- Windows 7 Ultimate x 64 Service Pack 1
- Windows 8
- Windows 8 x64
- Windows 8.1
- Windows 10

Application architecture

Kaspersky Security 9.0 for SharePoint Server includes the following components:

- **Administration Console**. This is a snap-in for Microsoft Management Console (hereinafter referred to as MMC). This component is designed for interaction with the application through an interface.

  You can install Administration Console separately from other application components. If you need to manage other components of the application, you can add computers with installed components to Administration Console. If several administrators work concurrently, Administration Console can be installed on each administrator's computer.

- **Security Server**. This component is designed for anti-virus protection of a SharePoint server (or server farm) and for scanning files, blogs, and wiki pages for unwanted content. Security Server is responsible for real-time protection, updating the application databases, background scanning of SharePoint servers, relaying data to Kaspersky Security Network services, and activating the application.

- **DLP Module**. This component is designed to protect SharePoint data against leaks. The DLP Module is part of Security Server and can be installed on a SharePoint server only together with Security Server. A separate key is required to use the DLP Module.

> Some Kaspersky Security settings are stored in the memory of third-party software (Active Directory® and Microsoft SQL Server®). Kaspersky Security is unable to guarantee security of such data. To prevent unauthorized changes to these settings, you have to ensure their security on your own.

The figure below shows an example of application deployment within the Microsoft SharePoint Server structure.

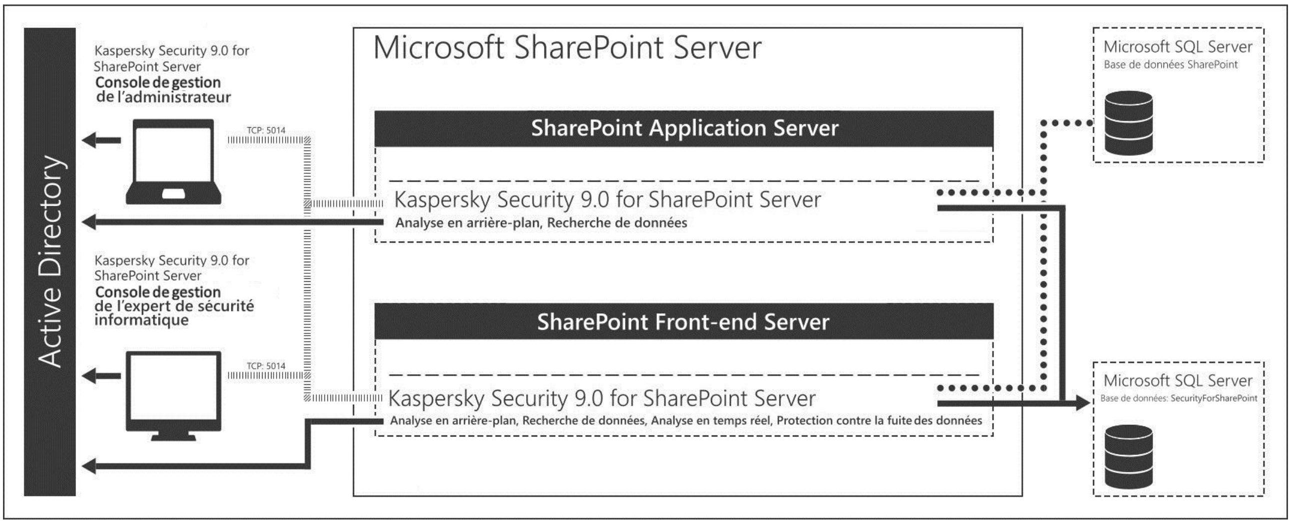
Active Directory
Kaspersky Security 9.0 for SharePoint Server
Console de gestion de l'administrateur
TCP: 5014
Kaspersky Security 9.0 for SharePoint Server
Console de gestion de l'expert de sécurité informatique
TCP: 5014
Microsoft SharePoint Server
SharePoint Application Server
Kaspersky Security 9.0 for SharePoint Server
Analyse en arrière-plan, Recherche de données
SharePoint Front-end Server
Kaspersky Security 9.0 for SharePoint Server
Analyse en arrière-plan, Recherche de données, Analyse en temps réel, Protection contre la fuite des données
Microsoft SQL Server
Base de données SharePoint
Microsoft SQL Server
Base de données: SecurityForSharePoint

Figure 1. Kaspersky Security for SharePoint Server deployment example

About information stored in the SQL database

The application saves the following information to the SQL database:

- Details of Security Server's operation:
  - The component's configuration
  - The component's operation statistics
  - Ready reports
  - Backup copies of documents.
- Details of DLP Module's operation:
  - The component's configuration
  - Information about user categories
  - The component's operation statistics
  - Ready reports

- Information about incidents (including files associated with incidents)
- Information about the progress of scan tasks.

Files associated with incidents and backup copies of documents are not encrypted. For security reasons (for example, to prevent unauthorized access or possible data leaks), you are advised to protect files in the SQL database on your own.

Information about incidents may increase the size of the database significantly. An information security specialist can archive incidents. This procedure allows minimizing the volume of data stored in the SQL database.

Role-based access restriction in Kaspersky Security for SharePoint Server

Kaspersky Security for SharePoint Server supports the roles of Administrator and Security Officer. Roles restrict users' rights of access to the application's features. The Administrator and the Security Officer use different features of the application to achieve their respective goals. The functions of these two roles do not overlap.

Two different sets of nodes are displayed Kaspersky Security Administration Console for the Administrator and for the Security Officer. The table below lists the main tasks for the Administrator and for the Security Officer, as well as nodes displayed in Administration Console for these two roles.

Table 2. Main tasks of Kaspersky Security roles

Role	Main tasks	Nodes in Administration Console
Administrator	• Configuring the anti-virus protection; • Configuring content filtering; • Scanning servers for viruses and unwanted content; • Application licensing; • Detecting false positives; • Reducing the workload on SharePoint servers.	• Control Center; • On-access scan; • On-demand scan; • Content filtering; • Backup; • Updates; • Notifications; • Reports; • Settings; • Licensing.
Security Officer	• Detecting confidential data on portals; • Protection of confidential data; • Data leak prevention; • Processing possible leakage incidents.	• Protection from Data leaks; • Categories and policies; • Incidents; • Search; • Reports.

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

- KSH Administrators (Administrator);
- KSH Security Officers (Security Officer).

You can create those groups manually before installing Kaspersky Security (see page 32). If the account under which Kaspersky Security is being installed, has the rights to create groups in Active Directory, groups will be created automatically when installing the application.

A user can combine the roles of Administrator and Security Officer. In this case, the user will have access to all of the application's features. If a user needs to combine both roles and use all of the features of Kaspersky Security, the corresponding account should be added to both groups in Active Directory. The account of the user who has installed the application will be added to both groups in Active Directory. Role assignment with the KSH Administrators and KSH Security Officers groups apply to all servers in a SharePoint farm.

Access rights for managing Kaspersky Security

Kaspersky Security installation and management are based on the access rights granted to the account under which all actions on the application are performed. The rights required for Kaspersky Security installation and management are listed below.

Rights for running Kaspersky Security services

The account under which Kaspersky Security services will be run, must have the following set of rights:

- Local administrator rights on the SharePoint servers on which Kaspersky Security is to be installed
- SharePoint Farm Administrator rights

The account for Kaspersky Security management must also have access to the SharePoint_Config and SharePoint_AdminContent_<GUID> databases, where <GUID> is a unique web app ID.

You can provide the account with access to these databases using one of the following methods:

- Assign the db_owner role to the account using Microsoft SQL Server Management Studio or the Microsoft SQL Server Management Studio Express utility (the account will have full access rights to these databases).
- Run the following script using Windows PowerShell™:

  ```
  $wa = Get-SPWebApplication <http://WebApp.domain.com>

  $wa.GrantAccessToProcessIdentity(<domain\KSH_User>)

  $wa.Update()
  ```

  `http://WebApp.domain.com` is the web address or GUID of the web application on the SharePoint portal, and <domain\KSH_User> is the name of the account created for managing Kaspersky Security.

The web application can be accessed through authentication of the specified account. This script must be run for every web app on the protected SharePoint portal to which you need to provide access.

Rights for installing Kaspersky Security

The account under which you run the application installation, must have the following set of rights:

- Local administrator rights on the computer on which Kaspersky Security is to be installed
- Rights for creating groups in Active Directory

  Without the rights for creating groups in Active Directory, the application cannot create role-based control groups automatically (see section "Role-based access restriction in Kaspersky Security for SharePoint Server" on page 26). If these rights have not been granted to the account, you have to create role-based control groups manually (see page 32).
- Rights for SQL database preparation.

Also, the account under which Kaspersky Security is to be installed must have access to the SharePoint_Config and SharePoint_AdminContent_<GUID> databases, where <GUID> is a unique web app ID.

You can provide the account with access to these databases using one of the following methods:

- Assign the db_owner role to the account using Microsoft SQL Server Management Studio or the Microsoft SQL Server Management Studio Express utility (the account will have full access rights to these databases).
- Run the following script using Windows PowerShell:

  ```
  $wa = Get-SPWebApplication <http://WebApp.domain.com>
  
  $wa.GrantAccessToProcessIdentity(<domain\KSH_User>)
  
  $wa.Update()
  ```

  `http://WebApp.domain.com` is the web address or GUID of the web application on the SharePoint portal, and <domain\KSH_User> is the name of the account created for managing Kaspersky Security.

The web application can be accessed through authentication of the specified account. This script must be run for every web app on the protected SharePoint portal to which you need to provide access.

When no access to the SharePoint databases is provided, the anti-virus settings of the SharePoint server cannot be defined. At the final step of installation, when the files are being copied and the components registered, the corresponding error message appears. When the error message appears, click the **Ignore** button in the dialog box and, when the installation finishes, reboot the ISS server using the command `iisreset / restart`.

Rights for SQL database preparation

Kaspersky Security uses the SQL database to store Backup configuration files and data. You can provide the account selected for SQL database preparation with access to the database using one of the following methods:

- Assign the account the sysadmin role on the SQL server (on which a database for Kaspersky Security management already exists or is to be created).

  Users with the sysadmin role can perform any actions on the SQL server. If the account has been assigned the sysadmin role, the database can be created automatically during the application installation.

- Assign the account the db_owner role for a database that was created manually (see section "Creating a database manually" on page 35).

  If the database was created manually before the application installation, you will need to specify this database in the SQL server connection settings during the application installation (see section "Step 5. Configuring the connection between Kaspersky Security and SQL database" on page 44). Users with the db_owner role can perform any actions on the database.

The account intended for SQL database creation and preparation will be used only when the Application Installation Wizard is running. It will not be used after installation of Kaspersky Security is complete.

Rights for managing Kaspersky Security

The account under which you intend to manage Kaspersky Security, must have the following set of rights:

- SharePoint Farm Administrator rights
- Read/write access for the <application installation folder>\Configurations path

  By default, the account that has been granted the local administrator rights on the computer, has the read/write access in this folder.

Also, the account under which you run Management Console must be added to the Active Directory group, which corresponds to the user role (KSH Administrators or KSH Security Officers) (see section "Role-based access restriction in Kaspersky Security for SharePoint Server" on page 26).

Kaspersky Security cannot be managed without this set of rights.

Installing and removing the application

This section provides instructions on how to install and remove the application, as well as information about system changes after installation of the application.

In this section

Preparing to install

Before preparing your computer for Kaspersky Security installation, make sure that the hardware and software on your computer meet the requirements for the Security Server and Administration Console (see page 19).

► *To prepare your computer for Kaspersky Security installation:*

1. Install all of the components required for the Kaspersky Security operation (if they are still missing):

   - Microsoft .NET Framework 3.5 SP1.

   - Microsoft Management Console 3.0 (MMC 3.0).

You can download these components by clicking the link in the welcome window of the Kaspersky Security installation package (see section "Step 1. Installing the required components" on page 41) and then install them. The computer must be restarted after Microsoft .NET Framework 3.5 SP1 installation. Continuing the application installation without restart may cause failures in the Kaspersky Security operation.

If Microsoft SharePoint Server is not installed on the computer, the application prompts you to install Administration Console alone. In this case, the Security Server and the DLP Module cannot be installed on this computer.

2. Create an account to run Kaspersky Security services and grant it all the relevant rights (see section "Access rights for managing Kaspersky Security" on page 28).

3. Create an account under which Kaspersky Security installation will be run, and grant it all the relevant rights (see section "Access rights for managing Kaspersky Security" on page 28).

   If no access rights for the SharePoint_Config and SharePoint_AdminContent_<GUID> databases are provided, the anti-virus settings of the SharePoint server cannot be defined. At the final stage of the installation, when the files are being copied and the components registered, an error message appears. When the error message appears, click the **Ignore** button in the dialog box and, when the installation finishes, reboot the ISS server using the command iisreset / restart.

4. If necessary, create a database manually (see section "Creating a database manually" on page 35) to store configuration files and Backup data.

   You can also use the databases created during the previous installation of Kaspersky Security. In this case, no additional actions are required.

   If the account intended to handle the SQL database has been assigned the sysadmin role on the SQL server on which the database is to be created, you can skip this step. If these rights have been granted, the database will be created by the Application Installation Wizard automatically.

   > Kaspersky Security does not provide channel encryption during data transmission between the server and the SQL database. To secure your data, manually encrypt data to be transmitted over communication channels.

5. Create an account for SQL database preparation and grant it all the relevant rights (see section "Access rights for managing Kaspersky Security" on page 28).

6. In Active Directory, create groups for role-based access to Kaspersky Security features (see section "Role-based access restriction in Kaspersky Security for SharePoint Server" on page 26). These groups can be created in any of the organization's domains. The group type is "Multipurpose". Group names:

   - KSH Administrators
   - KSH Security Officers

   If the account under which Kaspersky Security is to be installed, has the rights to create groups in Active Directory, you can skip this step. The groups will be created automatically during the application installation.

   > If you are installing Kaspersky Security on two servers one of which is located in the root domain, while the other is in a child domain, first install the application on the former server. Before starting installation on the second server, wait for automatic replication of Active Directory, or perform replication manually (preferred). This requirement is due to the fact that Kaspersky Security configuration data common to a group of Security Servers is stored in Active Directory. Installing several instances of the application in this configuration without performing Active Directory replication can cause configuration data duplication, which may lead to incorrect operation of the application.

7. Create an account to manage Kaspersky Security services and grant it all the relevant rights (see section "Access rights for managing Kaspersky Security" on page 28).

   Kaspersky Security cannot be managed without those rights.

   > Administration Console connects to the Security Server over TCP using port 5014. The port must remain open to allow management of the Security Server.

Upon finishing your installation preparations, you can proceed to Kaspersky Security installation (see section "Step 1. Installing the required components" on page 41).

Creating a database manually

► *To create a database manually, run the following SQL script:*

```
CREATE DATABASE [<database name>]

ON PRIMARY

(

NAME = [<name of database>_

<logical name of the primary data file> ],

FILENAME = '<full path to the primary data file>'

),

FILEGROUP [<name of database>_BACKUP_DATA_FILE_GROUP]

(

NAME = [<name of database>_BACKUP_DATA_FILE_GROUP],

FILENAME = 'full path to the secondary data file'

)
```

To manage the database that has been created manually, you must grant the relevant access rights to the account intended for database preparation (see section "Access rights for managing Kaspersky Security" on page 28).

Special considerations of installing the application

When Kaspersky Security is installed on a SharePoint farm, the application needs to be successively installed on all the SharePoint farm servers. When the installation completes on the first SharePoint farm server, you can use the Configuration Wizard to perform the initial setup of the application. The installation of Kaspersky Security on the other SharePoint farm servers uses the initial settings configured during installation of the application on the first SharePoint farm server.

If you plan to install the application on two servers one of which is located in the root domain and the other one in a subordinated domain, after completing installation on the first server and before starting installation on the second server wait for automatic replication of Active Directory or perform replication manually (preferred). This requirement is due to the fact that Kaspersky Security configuration data common to a group of Security Servers of Kaspersky Security is stored in Active Directory. Installing several instances of the application in this configuration without performing Active Directory replication can cause configuration data duplication, which may lead to incorrect operation of the application.

The process of Kaspersky Security installation is accompanied by the Setup Wizard. The Setup Wizard will prompt you to configure the installation settings. Follow the Wizard's instructions.

Upgrading from a previous version of the application

This section describes the procedure for upgrading from the previous version of the application. This section includes upgrade instructions and describes the specifics of upgrading Kaspersky Security on a standalone SharePoint server and on a SharePoint server farm.

In this section

About Kaspersky Security upgrades

Kaspersky Security 9.0 Maintenance Release 1 (build 9.1.45175) can be upgraded to version 9.0 Maintenance Release 2. Upgrades of earlier application versions are not supported. To run the application upgrade, the account under which Kaspersky Security is to be upgraded must have rights to handle SQL databases (see section "Access rights for managing Kaspersky Security" on page 28).

During the application upgrade process, Anti-Virus databases are rolled back automatically. For the safety of your computer, you are advised to start the database update after completing the application upgrade. Application functionality can change after update.

> Before upgrading Security Server for Kaspersky Security, you are recommended to complete all on-demand scan, report and database update tasks running on the server. Otherwise, these tasks are forcibly stopped prior to completion.

The following upgrade configurations of Kaspersky Security are available:

- Security Server and Administration Console installed on a standalone SharePoint server
- Security Server and Administration Console installed on a SharePoint server in a SharePoint farm environment.
- Administration Console only

During the upgrade of a separately installed Administration Console, tasks running on Security Server are not suspended. SharePoint server protection remains enabled.

When the application upgrade is started, the **I have read the KSN Statement and accept all of the conditions therein** check box is cleared automatically in Kaspersky Security settings. When the upgrade is complete, you can accept the KSN Statement and define the settings of KSN usage (see section "KSN Protection Settings" on page 116). The remaining Kaspersky Security settings are moved to the new version without any changes.

When upgrading Kaspersky Security 9.0 Maintenance Release 1 to version Kaspersky Security 9.0 Maintenance Release 2, all the settings of notification templates will be reset. We recommend that you restore the **Default** notification templates for all notification recipients when the upgrade is complete.

Other Kaspersky Security settings are transferred to the new version unchanged.

When upgrading Kaspersky Security 9.0 Maintenance Release 1 to version 9.0 Maintenance Release 2, failures may occur in the operation of the SharePoint Timer service. Errors in the Windows Event Log will indicate an operation failure. Text of error messages will start with the name of the SharePoint.Integration.Vsapi.Com.dll module. In this case, you will have to restart the SharePoint Timer service (see section "Restarting the SharePoint Timer service" on page 40). The SharePoint Timer service must be restarted on all the servers on which Kaspersky Security is installed.

Tips for upgrading Kaspersky Security on a SharePoint farm

When upgrading Kaspersky Security on a SharePoint server farm, it is recommended that you complete the upgrade in the shortest possible time frame.

When upgrading Kaspersky Security on a SharePoint server farm, it is not recommended to perform any operations with the application until the upgrade has been completed on all SharePoint farm servers.

If you need to resume using the application before an upgrade is completed on a SharePoint server farm, the version number of Security Server should comply when being added to Administration Console. You can add Security Server of the previous version to Administration Console that has not yet been upgraded, or you can add Security Server of the new version to the upgraded instance of Administration Console.

However, Security Server that has not yet been upgraded cannot be added to the upgraded instance of Administration Console.

Upgrading Kaspersky Security on a standalone SharePoint server or the first server in a SharePoint farm

When upgrading Security Server and Administration Console on the first server in a SharePoint server farm, or on a standalone SharePoint server, the following items are transferred to the new version:

- Active key and additional key that have been added before the application upgrade. The respective validity periods of the keys remain unchanged.
- Settings of Kaspersky Security that have been defined before the application upgrade.
- Objects moved to Backup before the application upgrade.
- Reports created before the application upgrade.

The application uses the application log to save the operation data of the Security Server version that has not yet been upgraded.

> Operation statistics of Security Server that have been collected before the application upgrade, will not be saved nor displayed in the **Control Center** node. Reports that have been created after the application upgrade, will not contain any information about the application's activity before the upgrade.

If you modify any settings of the upgraded Security Server on the first server in a SharePoint server farm, the settings that have been modified will be applied to other SharePoint servers. Security Servers that have not yet been upgraded continue running under the settings defined before the upgrade start.

Starting the application upgrade

► *To run an upgrade of Kaspersky Security deployed in any of the above configurations:*

1. If Kaspersky Security Administration Console is running on the computer for which you want to upgrade the application, close this Administration Console before starting the upgrade.
2. Run the file setup.exe in the distribution package of the application on the computer for which you want to upgrade Kaspersky Security.

   This opens the welcome window of the install package.

3. Click the **Kaspersky Security 9.0 for SharePoint Server** link in welcome window to launch the Setup Wizard.

4. Click the **Install** button in the welcome screen of the Setup Wizard.

   The automatic upgrade of the application now starts. When the upgrade completes, the final screen of the Setup Wizard opens.

5. To complete the upgrade and close the Setup Wizard, click the **Finish** button.

The upgrade completes. When the upgrade of Kaspersky Security 9.0 Maintenance Release 1 to version 9.0 Maintenance Release 2 is complete, you need to restart SharePoint Timer service (see section "Restarting the SharePoint Timer service" on page 40).

> During the upgrade, SharePoint server protection is disabled because all services under the application are suspended until the upgrade of Security Server for Kaspersky Security completes.

Restarting the SharePoint Timer service

SharePoint Timer needs to be restarted after Kaspersky Security 9.0 Maintenance Release 1 is upgraded to version 9.0 Maintenance Release 2.   The SharePoint Timer service must be restarted on all the servers on which Kaspersky Security is installed.

► *To restart the SharePoint Timer service:*

1. Run Windows PowerShell under the administrator account.

2. In the PowerShell environment, run the `Add-PSSnapin Microsoft.SharePoint.PowerShell` command.

   The Windows PowerShell snap-in will be added.

3. Run the `Get-SPTimerJob job-timer-recycle | Start-SPTimerJob` command.

SharePoint Timer will be restarted.

Application setup procedure

This section provides a step-by-step instruction for installation of the application.

In this section

Step 1. Installing the required components

► *To start the installation of Kaspersky Security,*

launch the setup.exe file from the application distribution package.

The welcome window of the Kaspersky Security installation package opens. In this window, you can perform one of the following actions:

- Download and install the .NET Framework 3.5 SP1   component (if the component is not installed);

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

- Download and install the Microsoft Management Console 3.0 component (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 program in earlier versions of Microsoft Windows Server, you need to update MMC to version 3.0.

- start the Setup Wizard by clicking the **Kaspersky Security 9.0 for SharePoint Server** link.

  If Microsoft SharePoint Server is not installed on the computer, the application prompts you to install Administration Console alone. In this case, Security Server and DLP Mpdule cannot be installed on the computer.

Step 2. Viewing the welcome screen and License Agreement

The welcome screen contains information about how to begin the installation of Kaspersky Security on your computer. To switch to the window containing the License Agreement, click the **Next** button.

The End User License Agreement is an agreement between the application user and AO Kaspersky Lab. Checking the box **I accept the terms of the License Agreement** means that you have read the License Agreement and accepted its terms and conditions. You can print the text of the License Agreement by clicking the **Print** button.

To continue to the next step of the Setup Wizard, click the **Next** button.

Step 3. Selecting the type of installation

You can select one of the following application installation options:

- **Typical**. This installation uses the default paths to the installation and data storage folders. The application installs all Kaspersky Security components. The Setup Wizard proceeds to the **Configuring the connection between Kaspersky Security and SQL database** step (see section "**Step 5. Configuring the connection between Kaspersky Security and SQL database**" on page 44).
- **Custom**. In the next window of the Setup Wizard, you can select the application components to be installed, and the installation and data storage folders. The Setup Wizard proceeds to the **Selecting the application components** step (see section "**Step 4. Selecting the application components**" on page 43).

Once the installation type is selected, the Setup Wizard proceeds to the next installation step.

Step 4. Selecting the application components

► *To select the application components to be installed and specify the paths to the installation and data storage folders:*

1. Select the application components that you want to install.

   You can install either Security Server (with or without the DLP Module) and Administration Console, or Administration Console alone. Only Administration Console is installed to manage Security Server of Kaspersky Security remotely on a different computer.

2. Click the **Browse** button, and in the window that opens specify the path to the installation folder.

   The full path to the default installation folder is displayed in the field **Destination folder**.

3. Click the **Browse** button, and in the window that opens specify the path to the data storage folder.

   The full path to the default data storage folder is displayed in the field **Data storage folder**.

   The data storage folder contains application runtime logs and application databases.

4. Click the **Reset** button if you want to cancel the paths to the installation and data storage folders that you specified and return to the default options.

5. Click the **Disk Usage** button if you want to view information about free space available on local drives required to install the selected components.

   The window that opens displays information about local drives.

6. To continue to the next step of the Setup Wizard, click the **Next** button.

Step 5. Configuring the connection between Kaspersky Security and SQL database

► *To configure a connection to link Kaspersky Security to an SQL database:*

1. 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.

   Click the **Browse** button opposite the **Name of SQL server** field to select the SQL server in the network segment in which the computer is located.

   > If the connection is to a remote SQL server, make sure that the SQL server is enabled to support TCP/IP as a client protocol.

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

   > If you install Kaspersky Security on a farm of SharePoint servers, make sure that all servers with the installed application use one and the same SQL database. To this end, identical values must be specified in the **SQL server name** and **Database name** fields when you install the application on all farm servers.

   The application can use one of the following databases:

   - The database created in advance by the SQL server administrator (see page 32).
   - The database created automatically by the Setup Wizard installer.
   - The database used by the previous version of the application (version 9.1.45175) – if you are reinstalling or upgrading the application.

     After being reinstalled or updated, the application uses the contents of this database: runtime reports, statistics, setup information. The configuration includes application settings that were change during the reinstallation / update of the application.

3. Select an account for use with the SQL server during installation of the application.

   - **Active account**. Current user account will be used then.
   - **Other account**. In this case, enter the name and password for the specified user account. You can also click the **Browse** button to select an account.

   The account must be assigned the necessary rights (see page 32) and sysadmin role on the SQL server specified in the **SQL server name** field.

4. To finish the configuration and continue to the next step of the Setup Wizard, click the **Next** button.

> Kaspersky Security does not provide channel encryption during data transmission between the server and the SQL database. To secure your data, manually encrypt data to be transmitted over communication channels.

Step 6. Select an account for running Kaspersky Security services

► *To select an account for running Kaspersky Security services,*

specify the name and password of the account in the **Account** and **Password** fields in the Setup Wizard window, or select an account by clicking the **Browse** button.

> To ensure proper operation of the application, the account must be assigned all the necessary rights (see page 32).

Step 7. Completing installation

► *To continue the installation:*

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

   It will initiate copying of the application files to the computer and registration of the components in the system. Once the files are copied and the components are registered in the system, the Setup Wizard will display a notification informing about completion of the application setup.

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

   If the application is installed on a standalone SharePoint server or the first server in a SharePoint farm, the Configuration Wizard starts automatically (see section "Getting started. Application Configuration Wizard" on page 49). The Configuration Wizard allows you to specify the initial application settings: activate the application, enable SharePoint server protection, and configure application database updates.

   If you are installing the application on the remaining servers of a SharePoint farm, the Application Configuration Wizard will not be started. The installation is now complete, and the Setup Wizard closes automatically.

   Kaspersky Security on these SharePoint farm servers uses the settings defined in the Application Configuration Wizard during setup on the first server of the SharePoint farm. Protection on subsequent servers of the SharePoint farm is enabled as soon as Kaspersky Security has been installed, but only if SharePoint farm server protection was enabled at the **Configuring the real-time protection** step of the Application Configuration Wizard (see the section "**Step 2. Enabling the anti-virus protection**" on page 50).

Changes in the system after installing the application

When Kaspersky Security is installed on the computer, the following changes are made:

- Kaspersky Security folders are created.
- Kaspersky Security are registered.
- Kaspersky Security keys are registered in the system registry.

In special cases, application behavior can be modified by means of special configuration files that have to be saved in the application folder. Contact Technical Support for more details.

Kaspersky Security folders

Table 3. Kaspersky Security folders created on the computer

Folder	Kaspersky Security files
%Kaspersky Security folder%; by default: • In Microsoft Windows 32-bit version – %ProgramFiles%\Kaspersky Lab\Kaspersky Security for SharePoint Server\ • In Microsoft Windows 64-bit version – %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security for SharePoint Server\	Executable files, configuration, and logs of Kaspersky Security (destination folder specified during installation).
• In Microsoft Windows 32-bit version – %ProgramFiles%\Kaspersky Lab\Kaspersky Security for SharePoint Server\data\ • In Microsoft Windows 64-bit version – %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security for SharePoint Server\data\	Updatable data of Kaspersky Security
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Kaspersky Security for SharePoint Server\	Shortcuts of Administration Console, Administrator's Guide, Kaspersky Security Uninstaller, and IFilter utility.
C:\Windows\assembly\GAC_MSIL\SharePoint.Integration.Vsapi.Com	File to integrate Kaspersky Security with SharePoint.

Kaspersky Security services

Table 4. Kaspersky Security services

Service	Purpose
KSHSecurityService	The main service of Kaspersky Security; it manages tasks and processes of Kaspersky Security.
KSHIntegrationService	Service to integrate Kaspersky Security with SharePoint and IFilters.
KSHAdministrationService	Service to manage Kaspersky Security and integrate it with the application configuration.

System registry keys

Table 5. System registry keys

Key	Purpose
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Web Server Extensions\AVScanner]	Registration of the Anti-Virus with SharePoint
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{2D4428D8-63EB-41f4-97C9-B8E240B6ED58}]	Configuration of the Anti-Virus for SharePoint
In the Microsoft Windows 32-bit version: [HKEY_LOCAL_MACHINE\SOFTWARE\Kaspersky Lab\Kaspersky Security for Microsoft SharePoint] In the Microsoft Windows 64-bit version: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Kaspersky Lab\Kaspersky Security for Microsoft SharePoint].	Kaspersky Security configuration settings
In the Microsoft Windows 32-bit version: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\SnapIns\FX:{44267241-A2B7-4ed2-82E6-BC127AA5CDD1}] In the Microsoft Windows 64-bit version: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MMC\SnapIns\FX:{44267241-A2B7-4ed2-82E6-BC127AA5CDD1}].	Administration Console MMC snap-in

Key	Purpose
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application\KSH8]	Windows Event Log source.
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\KSHAdministrationService] [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\KSHIntegrationService] [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\KSHSecurityService]	Kaspersky Security services

Getting started. Application Configuration Wizard

This section provides step-by-step instructions for preparing the application for use with the help of the Application Configuration Wizard.

You can close the Application Configuration Wizard by clicking the **Cancel** button in the welcome window of the Application Configuration Wizard, and perform the necessary configuration after starting Kaspersky Security.

In this section

Step 1. Activating the application

► *To activate the application:*

1. Click the **Add** button in the Application Configuration Wizard.
2. In the window that opens, specify the path to the key file (a file with the .key extension) and click the **Open** button.

   The key corresponding to the license that entitles the owner to use the entire functionality of Kaspersky Security for the specified time period will be added in the product then.

   > The key added during installation on the first SharePoint farm server is automatically used to install the application on subsequent SharePoint farm servers.

► *To remove the key,*

click the **Delete** button in the Application Configuration Wizard.

Step 2. Enable Anti-Virus protection

► *To configure the anti-virus protection settings for a SharePoint server or servers:*

1. Select the **Enable anti-virus protection** check box to enable anti-virus scanning of files as they are uploaded to the server or downloaded from the server to the user's computer.
2. Select the **Enable automatic database updating** check box if you want the application to update the anti-virus databases automatically as scheduled, or clear the check box if you want to run updates of the databases manually.

Step 3. Kaspersky Security Network

In the **Use of Kaspersky Security Network** window, you can view the Statement on the use of Kaspersky Security Network services for protection of your computer.

► *To participate in Kaspersky Security Network,*

select the **I accept the KSN Agreement and want to use KSN** check box if you have read the KSN Statement and accepted all of its conditions.

Step 3. Configuring the proxy server settings

In the **Configuring proxy server to retrieve updates and connect to Kaspersky Security Network** window of the Application Configuration Wizard, you can define the proxy server settings for Kaspersky Security.

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

1. Select the **Use proxy server** check box if you want the application to connect to Kaspersky Lab update servers via a proxy server.

2. Specify the proxy server address in the **Proxy server address field**.

3. Specify the proxy server port number in the **Port** field.

   The default port number is 8080.

4. If a password is required to access the proxy server, specify the proxy user authentication settings. To do this, check the **Use authentication** box and fill in the **Account** and **Password** fields.

   The application uses the specified proxy server to retrieve updates and connect to Kaspersky Security Network

To finish configuration of the application and proceed to the final step in the Configuration Wizard, click the **Next** button.

Step 5. Completing application configuration

► *To stop the application configuring:*

1. If you want Kaspersky Security Administration Console to run automatically after closing the Configuration Wizard, leave the **Start Management Console after the Application Configuration Wizard finishes** check box selected.

2. To finish the configuration of the application and exit the Configuration Wizard, click the **Finish** button.

   The Configuration Wizard closes. If the **Start Management Console after the Application Configuration Wizard finishes** check box has been selected, Administration Console starts as soon as the Configuration Wizard closes.

Restoring the application

If the application malfunctions (due to a damaged executable file of the application or the application databases, or a fault in the operation of VS API interceptor), you can restore the application using the Setup Wizard.

During restoration, the installer replaces the executable files and libraries used by Kaspersky Security with the files contained in the Distribution, application databases – databases in the Distribution, and replaces the registration of VS API interceptor.

The application's configuration and event logs are saved during the restoration process.

► *To restore Kaspersky Security:*

1. Launch the setup.exe file from the application distribution package.

   This opens the welcome window of the install package.

2. Click the **Kaspersky Security 9.0 for SharePoint Server** link in welcome window to launch the Setup Wizard.

3. Click the **Next** button in the welcome screen of the Setup Wizard.

   This opens the **Change, Restore, or Remove the Application** window.

4. In the **Change, Repair or Remove the application** window, click the **Restore** button.

   This opens the **Restoration** window.

5. In the **Restoration** window, click the **Repair** button.

   The process to replace the executable files, libraries, and databases of the application and register VS API interceptor begins.

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 delete Kaspersky Security from the computer using:

- Standard Microsoft Windows tools to install/uninstall applications.
- Using the Setup Wizard.

> To uninstall Kaspersky Security from the SharePoint farm, the application must be deleted from each SharePoint farm server.

► *To uninstall Kaspersky Security using the Setup Wizard:*

1. Launch the setup.exe file from the application distribution package.

   This opens the welcome window of the install package.

2. Click the **Kaspersky Security 9.0 for SharePoint Server** link in welcome window of the install package to launch the Setup Wizard.

   This opens the start window of the Setup Wizard.

3. In the start window of the Setup Wizard, click the **Next** button.

4. In the **Change, Restore, or Remove the Application** window click the **Remove** button.

5. In the **Uninstallation** window, confirm your choice by clicking the **Remove** button.

   The process of removing application files from the computer and unregistering application components begins.

6. If you are removing the application from a standalone SharePoint server or from the last server of a SharePoint farm, once the files have been removed a window appears prompting you to delete the application database. Select one of the following operations in this window:

   - If you want to delete the database containing the application configuration, Backup and statistical data, click **Yes**.

     > To delete the database, the account under which the removal process is running must possess the db_owner role for this database. If the account does not possess this role, in the window that appears click **No**. When Kaspersky Security is uninstalled, you need to delete the database manually.

   - If you do not want to delete the database in order to use the data stored in it for subsequent application re-installations, click **No**.

Application licensing

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

In this section

About the End User License Agreement

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

Carefully review 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 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.

You can add a key to the application by using 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.

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).
- Obtain a key file on the Kaspersky Lab website (https://activation.kaspersky.com/) based on your existing activation code.

About data provision

To increase the protection level, by accepting the terms of the License Agreement, you agree to provide the following information to Kaspersky Lab in automatic mode:

- Checksums of processed files (MD5)
- Data on the Kaspersky Security version currently in use

If an error occurs during Kaspersky Security installation, you agree to automatically supply Kaspersky Lab with information about the error code, application installation package currently in use, and the computer on which installation is being performed.

To detect new information security threats and their sources, as well as to increase the protection level of information stored and processed using your computer, when you accept the KSN Statement, you agree to participate in Kaspersky Security Network (see section "About participation in Kaspersky Security Network" on page 115) and transmit the following information to Kaspersky Lab in automatic mode:

- Information about phishing scan
    - Web address or IP address (IPv4 and IPv6 versions supported) of the phishing / malicious URL
    - Information about all phishing / malicious links and action taken on such web addresses
    - Web address or name of the company targeted in the phishing attack
    - Application installation ID
    - Application version
    - Version of the installed operating system, including the versions of installed updates
- Spam scanning details:
    - IP address of the sender of an email message being scanned
    - Check sums (SHA1) of email addresses, which contain data on the size and priority of email messages being sent
    - Check sums (MD5) of graphic objects attached to an email message
    - Check sum (MD5) of the name of a file attached to an email message
    - Technical details describing the method that the application uses to detect a suspicious email message, and duration of network request execution during a scan
    - Result of an email message scan and final spam rate of this message

    - Web addresses contained in a message being scanned, with deleted passwords, including the IDs for detection of different web addresses in the body of the same message
    - Names of content filtering categories by which unwanted content has been detected, as well as respective content topics
    - List of Heuristic Analyzer categories that have triggered during a scan
    - Short text signatures for email message text (irreversible text compression that does not allow restoration of the original text while the latter has not been transmitted) to filter known spam distribution lists and receive the application's verdict on them
    - Names of first-level domains from message text, unrestorable hash sum of the names of domains from the header of an email message being scanned, number of IP addresses (IPv4 and IPv6) in the header, and criterion of an address's belonging to a local or external network as related to the computer location network
    - Anti-Spam component stack and code of error in case one occurs

- Information for detection of emerging information security threats and threats that are hard to detect, together with their respective sources, intrusion threats, and for swift actions on increasing the level of protection of information stored and processed using this computer:
    - Version of installed operating system, including the versions of installed updates
    - Name of the installed Kaspersky Lab application, as well as the version and internal ID of the application installation
    - ID of the device on which the Kaspersky Lab application is installed
    - Check sums of files being processed (MD5, SHA2-256)
    - Check sum (MD5, SHA1) of the email addresses of the sender and the recipient of a suspicious email message
    - Name and size of an object being scanned, as well as check sums (MD5, SHA2-256), file type ID of the object being scanned, date and time of the object scan, web address and IP address at which the object was downloaded, and information about the object emulation

- Version of the currently used anti-virus databases
- ID of the anti-virus databases that the application uses to make a verdict on an object, name of a threat according to the Kaspersky Lab classification
- Sequence of actions to take on files during scans
- ID of the scan task within which an object was scanned
- Name of first-level domains from web addresses in email messages being scanned
- Code of error in an object scan in case one occurs
- Number of IP addresses (IPv4 and IPv6) in the header of an email message being scanned
- Information about files that are stored (or were stored earlier) on your computer, including the path to each of them, check sum (MD5, SHA2-256, SHA1), size, attributes, version, digital signature, web address and IP address at which a file was downloaded, and the check sums (MD5, SHA2-256, SHA1) of the process that generated the file
- Information about processes running in the system (process ID (PID), process name, details of the account under which the process has been run, application and command that have run the process, full path to process files and command line, description of the product to which the process belongs, including the product name and the publisher details, as well as information about currently used digital certificates and information required to verify them or indication of the absence of a digital signature of the file), as well as information about modules loaded into processes, including their names, sizes, types, check sums (MD5, SHA2-256), and paths
- Check sums (MD5, SHA2-256) of a process file or service file, file name and size, path to the file, names and paths to files that the process has accessed, names and values of registry keys that the process has accessed, RAM dumps, web addresses and IP addresses that the process has accessed, account under which the process is running, name of the computer on which the process is running, headers of process windows

- Unique license ID, license expiration date and license type, information about the versions of the operating system installed on the computer and its service packs, and local time

- Information about events in system logs, including event time, name of the log in which the event was detected, event type and category, name of the event source and its description

- Information about network connections, including version and check sums (MD5, SHA2-256, SHA1) of the file of a process that opened the port, path to the process file and its digital signature, local and remote IP addresses, numbers of the local and remote connection ports, connection status, and port opening time

- Check sum (MD5) of a file being scanned, web address at which the reputation is requested for, type of the detected threat according to the Kaspersky Lab classification, ID and version of the threat-related record in the anti-virus database

- If a potentially malicious object is detected, the user provides information about process memory data, elements of the system object hierarchy (ObjectManager), UEFI BIOS memory data (scanning subsystems), names and values of registry keys.

In order to improve the application operation, you agree to provide the following information to Kaspersky Lab:

- Information about the versions of the operating system (OS) installed on the computer and installed service packs, the version and check sums (MD5, SHA2-256) of the OS kernel file, and the OS operation mode parameters

- Version of the application component, which performs the update, update task type ID, application status after the update task completion, and update error code in case one occurs

- Information about software installed on the computer, including names of applications, names of software publishers, and information about files of installed software components (check sums (MD5, SHA2-256), size, version, and digital signature)

- Information about hardware installed on the computer, including type, name, model, firmware version, and characteristics of built-in and connected devices

- Information about the operating system at the moment of a crash: name and version of the driver, which caused a BSOD, bug check code and its parameters, driver failure stack, type ID of the detected memory dump generated at the failure occurrence, indication of the OS session duration longer than 10 minutes before a BSOD or an unexpected power-off, unique ID of the OS memory dump, BSOD date and time, reports of software drivers from the memory dump (error code, module name, name of the source code file, and string in which the error occurred), full name of the OS kernel build, name, localization, and version of the application in which the failure was detected, error number and description from the log of the application for which the failure was detected, information about an exceptional error in the application, application failure address in module offset format, name and version of the module of the application in which the failure occurred, application failure indication in the software plug-in, failure stack, application runtime before the failure occurred, software failure detection method (driver interceptions, traffic processing, or number of waiting workflows), and name of the process, which initiated the interception or traffic exchange, which, in turn, caused the software failure
- Information about the last unsuccessful OS restart in case one occurs, including the number of unsuccessful restarts

Kaspersky Lab protects any received information pursuant to the legal requirements and effective Kaspersky Lab rules. Kaspersky Lab uses any collected information in depersonalized format and as general statistics only. General statistics are automatically generated using original collected information and do not contain any private data or other confidential information. Originally collected information is cleared as it is accumulated (once per year). General statistics are stored indefinitely.

> Participation in Kaspersky Security Network is voluntary. You can opt out of participating in Kaspersky Security Network at any time (see section "KSN Protection Settings" on page 116). No personal data of the user is collected, processed, or stored.

Any information about data that the application sends to Kaspersky Lab can be obtained through the KSN Statement.

Activating Security Server

Security Server activation lets you use the full functionality of Anti-Virus protection and Content filtering and update application databases.

► *To activate Security Server:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Licensing** node of the relevant server.
3. Click the **Add** button in the **Active key** section.
4. In the window that opens, specify the path to the key file (a file with the .key extension) and click the **Open** button.

The application adds the Security Server key corresponding to the license.

The appearance of the **Active key** section changes. The section displays the following information:

- **Key status**. Details of the active Security Server key.
- **Key**. A unique alphanumeric sequence required to receive technical support from Kaspersky Lab.
- **License type**. Trial or commercial.
- **Representative**. Name of the representative of the company that executed the agreement to purchase the application.
- **Number of users**. The maximum number of employees with access to the SharePoint server protected by the application.
- **Expiration date**. The date when the Security Server license expires.

If you add a key on a server in a farm, the **Active key on the servers of the farm** table appears in the workspace of the **Licensing** node. The table contains a list of servers belonging to the farm and information about the status of keys on these servers.

> If Kaspersky Security is installed on a standalone SharePoint server, the key status details are displayed in the **Licensing** section in the workspace of the **Control Center (<Server name>)** node.

Activating the DLP Module

DLP Module activation enables the security officer to use the full functionality of the DLP Module and manage Data Leak Prevention.

> The DLP Module can be activated after activating Security Server. The DLP Module key validity period may not exceed the Security Server key validity period.

► *To activate the DLP Module:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Licensing** node of the relevant server.
3. In the **Active key for DLP Module** section, click the **Add** button.
4. In the window that opens, specify the path to the key file (a file with the .key extension) and click the **Open** button.

The application adds the DLP Module key corresponding to the license.

The appearance of the **Active key for DLP Module** section changes. The section displays the following information:

- **Key status**. Details of the active DLP Module key.
- **Key**. A unique alphanumeric sequence required to receive technical support from Kaspersky Lab.
- **License type**. Trial or commercial.
- **Representative**. Name of the representative of the company that executed the agreement to purchase the application.

- **Number of users**. The maximum number of company employees with access to management of Data Leak Prevention.
- **Expiration date**. DLP Module license expiration date.

Information on the DLP Module license is displayed in the **Protection Center** node on all servers.

Application functionality is limited when the DLP Module license expires. The application stops scanning files in real time as they are uploaded to SharePoint, creating new incidents, and searching for data belonging to specific categories. The security officer can view information about previously created incidents, create categories, policies and reports. After the Security Server license has expired, the application stops updating DLP Module databases.

Replacing a key

You can replace an active key with a key that has a longer validity period or allows more users of Kaspersky Security (if any).

Replacing an active key does not interfere with on-access scans, on-demand scan tasks, or database updates.

► *To replace the active key for Kaspersky Security:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Licensing** node.
2. Click the **Replace** button in the workspace.
3. In the displayed **File name** dialog specify path to the key file (file with the .key extension) and click **Open**.

► *To replace an additional key:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Licensing** node.
2. In the workspace, click the **Replace** button in the **Additional key** section.
3. In the displayed **File name** dialog specify path to the key file (file with the .key extension) and click **Open**.

Removing a key

► *To remove a key for Kaspersky Security:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Licensing** node.
2. In the workspace, click the **Delete** button in the **Active key** or **Additional key** section.

When Kaspersky Security is installed on a SharePoint farm and a key is removed from one SharePoint server within the farm, it is also removed from all servers of the SharePoint farm.

Getting started

This section provides information about how to run Kaspersky Security and add SharePoint servers with installed Security Server to Administration Console.

In this section

Starting Administration Console

The services of Kaspersky Security start automatically during the operating system start-up. Administration Console is started manually.

► *To start Administration Console, perform the following steps:*

1. In the **Start** menu select **Programs.**
2. Select the **Kaspersky Security 9.0 for SharePoint Server** folder in the list of programs.
3. Select **Kaspersky Security 9.0 for SharePoint Server** in the menu.

When Administration Console starts, the snap-in of Kaspersky Security connects to Microsoft Management Console, so the console tree displays the application icon and the node of **Kaspersky Security 9.0 for SharePoint Server**.

When Administration Console is running, you can add servers on which Security Server has been installed (hereinafter referred to as "*Protected servers*"), to Administration Console (see the section "Adding protected servers to Administration Console" on page 69).

> The application records information about starts and stops of Administration Console to Windows Event Log. A record contains information about the time of a start / stop of Administration Console, as well as the user who initiated those activities.

Adding protected servers to Administration Console

► *To add protected servers to Administration Console:*

1. Start Administration Console.
2. Select in Administration Console tree the node of **Kaspersky Security 9.0 for SharePoint Server**.
3. In the workspace, click the **Add server** button.
4. Select the appropriate option in the displayed dialog:
   - **Local**. The application adds to Administration Console the SharePoint server on which Administration Console and Security Server are installed. This is the default option.
   - **Remote**. The application adds to Administration Console the SharePoint server on which Security Server is installed. If you select this option, use one of the following methods to specify the server name:
     - Click **Browse** and select the computer from the list in the window that opens.
     - Enter the server name manually as an IP address (in IPv4 or IPv6 notation) or DNS name.
5. Click the **OK** button.

The server will be added to Administration Console and shown in the nodes tree.

If Kaspersky Security is installed on a farm of SharePoint servers, you can add any server of the farm to Administration Console.

Checking protection of SharePoint servers

This section describes how to check the protection level of Security Servers using Administration Console, i.e., how to view the licensing details, the status of application modules, as well as the statistics on objects scanned and threats detected.

In this section

Viewing SharePoint server protection status details

Details of the protection status, results of the databases updates, and the license status are displayed in the Control Center node for all Servers added to Administration Console.

The **Events and statistics** tab displays the following information about the protection status:

- Protection of farm servers (see page 72)
- Anti-virus settings of SharePoint (see page 73)
- Security Server license (see page 73)

- DLP Module license (see page 73)
- Database update (see page 74)
- Protection of farm servers (see page 76)
- Statistics (see page 76).

The **List of farm servers** tab displays a table with a list of SharePoint servers included in the farm, and information about the protection status and the update status of Kaspersky Security databases on all of the servers. The table contains the following information:

- Server name.
- Information on the current status of Anti-Virus protection and Content filtering on each server.

  Possible values of the **Protection status** column:

  - *Protection is enabled*. The component is enabled and is running properly.
  - *Anti-virus scan / Content filtering is disabled*. Anti-Virus scan and / or Content filtering is disabled.
  - *Anti-Virus Protection and Content Filtering errors*. Anti-Virus scan and / or Content filtering is enabled, but documents cannot be scanned due to license or database-related errors or other errors in the operation of Kaspersky Security. In this case, the **Protection status** column contains information about the error.
- Information on the current status of the DLP Module on each server;

  Possible values of the **DLP module** column:

  - *Running*. The DLP Module is enabled and is running properly.
  - *Disabled*. The DLP Module is installed but not enabled.
  - *DLP Module not installed*.
  - *Scan error*. The DLP Module is enabled, but documents cannot be scanned due to license or database-related errors or other errors in the operation of Kaspersky Security.

- Status of the last database update on the server.

  Possible values of the **Status of the last update** column:

  - *Databases are up to date. Update is not required*. The most recent update was successful. Databases were updated in the past 24 hours and are not corrupted.
  - *Databases are out of date. Update required*. Databases were not updated in the past 24 hours.
  - *Databases corrupted. Update required*. Database files are missing or corrupted and cannot be read by the application.
  - *Error updating databases*. The last database update attempt ended in an error. The column also contains the error description.

> If Kaspersky Security is installed on a standalone SharePoint server, the **List of farm servers** tab is not displayed.

Information about server protection

The **Protection of farm servers** section shows the current version of the application and the status of its components. The following component statuses are possible:

- *Enabled*. The component is enabled and runs correctly on all SharePoint farm servers.
- *Disabled*. The component is disabled on all the servers in the SharePoint farm.
- *Protection errors*. Errors have been detected in the operation the component on at least one of the SharePoint farm servers. The section contains a description of any errors that occur.
- *Unknown*. The status of Anti-Virus protection / Content filtering on at least one of the SharePoint farm servers is unknown.

Anti-virus settings of SharePoint

The **Anti-virus settings of SharePoint** section displays information about the scan settings defined on the SharePoint server (see the section "Kaspersky Security operation depending on the SharePoint server settings" on page 82). If anti-virus protection is disabled on the SharePoint server, Kaspersky Security does not perform Anti-Virus scanning and Content filtering in real time.

Application licenses

Depending on the application components installed on the SharePoint server, the workspace may display the following sections with licensing information:

- **Security Server license**;
- **DLP Module license**.

The **Key status** field displays the details of the active key. Available field values:

- *Current license*. A key has been added, and the license has not expired.
- *Errors on some farm servers*. Licensing errors or violations have been detected on at least one of the SharePoint farm servers (for example, a key is missing or blacklisted). The error description is displayed in red, and the section itself is highlighted in orange.
- *Key is missing.* No key has been added, and Administration Console is deployed on a standalone SharePoint server.

The **Expiration date** field displays the expiration date of the license.

> If the number of days remaining on the license is less than the number of days specified in the **Notifications** node, the expiration date in the field is displayed in red. You are advised to add an additional key in the **Licensing** node before the current license expires.

The **Additional key** field contains information about the availability of an additional key. Available values:

- **Added**. An additional key has been added, and the validity period of the active key has not expired yet.
- **Not added**. One of two possibilities:
  - an additional key is not added;
  - an additional key is installed, but the active key has expired.

The **Users** field contains information about the maximum number of company employees with access to a SharePoint server protected by the application.

The **Functionality** field contains information on available application features. Available field values:

- **Full functionality**. No limitations are imposed on the operation of Kaspersky Security.
- **The license expired. Database updates and technical support are not available**. The application does not update Anti-Virus protection, Content filtering, and DLP Module databases. To download the latest databases, you have to replace the key (see section "Replacing a key" on page 66).
- **Management only**. No key is installed, or the trial license has expired. Only management of Kaspersky Security is available. Anti-Virus protection and Content filtering are not performed, and updates are not available.
- **Update only**. The key is in the black list. Only database updates are available. Anti-virus scanning and content filtering are not performed.

Database update

The **Database update** section shows information about the current state of the anti-virus databases, the date of the last update, and the number of records in the databases.

The **Status** field displays information about the status of databases currently in use by Kaspersky Security.

If Kaspersky Security is installed on a SharePoint farm, the **Status** field can take the following values:

- *Databases are up to date on all farm servers*. Databases used on all SharePoint farm servers were updated in the past 24 hours and are not corrupted.
- *Databases outdated on some farm servers*. Databases were not updated in the past 24 hours.
- *Databases corrupted on some farm servers*. Databases are missing or corrupted, and cannot be read by the application on at least one SharePoint farm server.

If Kaspersky Security is installed on a standalone SharePoint server, the **Status** field can take the following values:

- *Databases are up to date*. Databases were updated in the past 24 hours and are not corrupted.
- *Update required*. Databases were not updated in the past 24 hours.
- *Databases corrupted*. Databases are missing or corrupted and cannot be read by the application.

The **Last update status** field displays the date and result of the most recent update of the databases. If an error occurred during the last database update, the field contains a description of the error. In this case, the **Database update** section is highlighted in orange, and the description of the error is displayed in red.

If Kaspersky Security is installed on a standalone SharePoint server, the section displays the **Last update** field, which contains the date and time of the most recent attempt to update the databases.

The **Release date and time** field shows the release date of the earliest database on all SharePoint farm servers. If the databases are out of date, the date is displayed in red. In this case, it is recommended that you go to the **Updates** node and update the application databases.

The **Records count** field contains information about the total number of records in the databases on the server since the time of the first update.

Protection of SharePoint farm servers

The **Protection of farm servers** section displays information about the current protection status of servers in the SharePoint farm.

SharePoint farm servers that have not accessed the database within the past 60 seconds are considered inactive by the application. The number and list of such servers are shown in this section. Detailed information about why the database was not accessed is displayed in a table on the **List of farm servers** tab.

> If Kaspersky Security is installed on a standalone SharePoint server, the **Protection of farm servers** section is not displayed in the workspace of the **Control Center (<Server name>)** node.

Statistics

The **Statistics** section contains statistics on the application's operation for the last week. The graph presents the following information about the number of positives returned by application components, the number of threats detected, files blocked, and clean files:

- ANTI-VIRUS PROTECTION:
  - **Total files**. The total number of files that are infected, probably infected, corrupted, password-protected, or clean, and files that returned an error during Anti-Virus scanning.
  - **Threats**. The number of malicious objects detected in scanned files.
  - **Excluded**. The number of files excluded from the scan scope.
  - **Non-infected.** The number of files scanned by the application and recognized as not infected.
  - **Other**. Files that do not match any other categories. The group includes, for example, files not scanned because of key errors or files that have caused errors while being processed.

- CONTENT FILTERING:
  - **Total**. The total number of files and SharePoint web objects that caused content filtering incidents (by content, by file type and format, and masks of unwanted file names, files with *Non-infected* status, and files that returned content filtering errors).
  - **Files with unwanted content**. The number of files found by Content filtering to contain unwanted words or phrases included in Kaspersky Lab categories and custom categories. You can configure custom categories in content filtering settings (see section "Configuring Content filtering" on page 101).
  - **Web objects with unwanted content**. The number of SharePoint web objects that have been found by Content Filtering to contain unwanted words or phrases included in Kaspersky Lab categories and custom categories, and the number of web objects found to contain malicious or phishing URLs.
  - **Files in unwanted formats**. Number of files in unwanted formats.
  - **Found clean**. The number of files that are free from unwanted content (with the names and formats not matching the specified masks of unwanted file names and formats), malicious or phishing URLs.
  - **Other**. Files that do not match any other category including files unprocessed because of errors.

Default protection

The protection status of the SharePoint server depends on the settings defined in the Application Configuration Wizard during installation. A detailed description of the Application Configuration Wizard is provided in the *Installation Guide for Kaspersky Security 8.0 for SharePoint Server*.

If the **Enable Anti-Virus protection** check box was selected in the Application Configuration Wizard during setup on the first SharePoint server, the application components are launched in the following mode at application startup:

- On-access scan:
    - Anti-Virus scan is enabled;
        - Action on infected and probably infected files: Disinfect;
        - Action on corrupted files and password-protected files: Skip;
    - Content filtering is enabled.
- On-demand scan:
    - On-demand scan tasks are not created. On-demand scan is not performed.

If the **Enable Anti-Virus protection** check box was cleared during application installation, the Anti-Virus scan and Content filtering components are disabled at application startup, and on-demand scanning is not performed.

On-access scan

This section provides information about how to scan SharePoint files and web objects in real-time mode (i.e., immediately after users access them). The section describes the operating mechanism of on-access scanning and provides instructions on how to define the scan settings.

In this section

About on-access scan

Real-time protection is an operation mode of Kaspersky Security in which objects are scanned for malicious code and web objects are scanned for unwanted web content in real-time mode. The application scans objects when they are transferred to a Server, modified, or downloaded from a Server to a user's computer.

Kaspersky Security scans the following objects:

- Files uploaded by the user to the SharePoint server;
- Files copied from the SharePoint server to the computer;
- SharePoint web objects (such as wiki pages and forums hosted on the SharePoint server) when they are created or modified.

When the real-time protection is enabled, Kaspersky Security performs the following actions:

- Anti-Virus scans of files in accordance with the currently set scan exclusions (see the section "Creating on-access anti-virus scanning exclusions" on page 84).
- Scanning for unwanted file formats and unwanted file names (see section "Configuring additional settings for on-access Content filtering" on page 87);
- Scanning of files and SharePoint web objects for unwanted content (see section "Configuring additional settings for on-access Content filtering" on page 87).
- Checking of links in web content against a database of malicious and phishing web addresses (see section "Enabling and disabling web content scanning for phishing" on page 90).

The application performs one type of scan:

- If a file was blocked during Content filtering, the application does not perform a virus scan on this file.
- If a file was blocked during a virus scan, the application does not scan its contents.

Non-infected objects are passed on to the user, while objects that contain threats or possible infection are processed in accordance with the currently defined protection settings (see the section "Configuring object processing rules for on-access scanning" on page 85).

Status labels assigned to files following on-access scan

Based on the results of on-access scanning, the application assigns one of the following status labels to the file:

- *Not infected*. No threats detected in the file.
- *Infected*. A file a segment of whose code fully matches a code segment of a known threat.

- *Probably infected*. A file whose code contains a modified segment of code of a known threat, or a file resembling a threat in the way it behaves.
- *Password-protected*. A password-protected archive.
- *Corrupted.* The file cannot be read by Kaspersky Security.

Based on the results of content filtering, the application assigns one of the following status labels to the file:

- *Allowed*. There is no unwanted content in the file.
- *Forbidden format*. The file has an unwanted format.
- *Forbidden mask*. The file name contains an unwanted mask.
- *Forbidden content*. The file has been found to contain unwanted words and phrases.

Based on the results of content filtering, the application assigns one of the following status labels to the SharePoint web part:

- *Allowed.* The SharePoint web object does not contain unwanted content, malicious or phishing URLs.
- *Forbidden content*. The SharePoint web object has been found to contain malicious / phishing URLs or unwanted content.

About phishing scan

Phishing scan is a feature of Kaspersky Security designed to protect the user's personal data.

While scanning the content of SharePoint web objects, the application checks links against lists of malicious and phishing URLs.

Checking links against the list of malicious URLs allows the application to detect URLs redirecting to infected websites. Malicious URLs can be contained in the text of messages disguised as ads. The ad text prompts you to find out more about a product or service by clicking a link. The link takes you to a website with viruses, and the computer gets infected. The computer is infiltrated by viruses and malware that can access your private data and relay it to criminals.

By checking links against the list of phishing web addresses, the application is able to detect links redirecting to fraudulent websites. A phishing attack can be disguised, for example, as an email message from your bank with a link to its official website. The link takes you to an exact copy of the bank's website where you can even see the bank site's address in the browser despite actually being on a spoofed website. From this point forward, all of your actions on the site are tracked and can be used to steal your private data.

A phishing scan of SharePoint web objects detects malicious and phishing URLs embedded in the text of web objects. Malicious and phishing URLs are designed to steal your personal data or information entered in a web form. The application performs a phishing scan when a SharePoint web object is created or modified. If the phishing scan detects at least one web address appearing on lists of malicious and phishing ones, the application assigns the *Phishing* status to the web object.

When detecting a malicious or phishing link in a SharePoint web object, the application performs the action configured in the **Content filtering** section (see the section "**Configuring object processing rules for on-access scanning**" on page 85). If the action is set to **Block**, the application shows a dialog saying that web content cannot be created or modified.

To protect SharePoint servers against phishing, the application uses a list of addresses of web resources that have been labeled as malicious or phishing links by Kaspersky Lab. The database is regularly updated and is part of the Kaspersky Security delivery kit.

You can use the *Kaspersky Security Network service* for additional protection of SharePoint servers against phishing (see the section "*About participation in Kaspersky Security Network*" on page 115). It uses cloud computing technology that provides up-to-the-minute information about threats before they have been included in Kaspersky Lab anti-phishing databases.

Kaspersky Security operation depending upon the SharePoint server settings

The operation of Kaspersky Security in on-access scan mode depends on the values of the anti-virus settings of SharePoint.

Table 6. Anti-virus settings of SharePoint

SharePoint setting	Value	Impact on the operation of Kaspersky Security
Scan files being uploaded to SharePoint	Check box selected	Kaspersky Security can scan files that are uploaded to SharePoint websites. The application performs on files actions that have been defined in the anti-virus protection settings.
	Check box cleared	Anti-virus protection of files uploaded to SharePoint websites is not available.
Scan files being downloaded from SharePoint	Check box selected	Kaspersky Security can scan files downloaded from SharePoint websites. The application performs on files actions that have been defined in the anti-virus protection settings.
	Check box cleared	Anti-virus protection of files uploaded to SharePoint websites is not available.
Allow users to download infected files	Check box selected	Kaspersky Security cannot block and disinfect files that users access. The application skips infected files.
	Check box cleared	The **Attempt to disinfect infected files** setting impacts the operation of Kaspersky Security.
Attempt to disinfect infected files	Check box selected	Kaspersky Security can disinfect infected files when they are accessed by users. If the application cannot disinfect a file, it blocks the file.
	Check box cleared	Kaspersky Security can block infected files when they are accessed by users.

The anti-virus protection settings of Kaspersky Security may conflict those of SharePoint. For example, if the **Allow users to download infected files** check box is selected in the anti-virus protection settings of SharePoint while the **Block** action is selected in the anti-virus protection settings of Kaspersky Security, the user will be able to download an infected file. Before downloading, the web browser window shows a warning message informing that Kaspersky Security recommends you to avoid downloading that file.

When a conflict arises between the anti-virus protection settings of Kaspersky Security and the anti-virus settings of SharePoint, the latter ones will have the higher priority.

Configuring basic scan settings

► *To define the general settings of real-time protection:*

1. In the Administration Console tree, select the Server for which the real-time protection should be configured.
2. Select the **On-access scan** node.
3. In the workspace, select the **General** tab.
4. Select the **Move files to backup** check box if you want Kaspersky Security to add to Backup copies of files that have been blocked by Anti-Virus scanning and Content Filtering.
5. To limit the size of files to be scanned, select the **Exclude from scanning any files larger than** check box and specify the maximum size of files to be scanned (in MB). The default value is 10 MB.
6. Click the **Save** button.

Creating on-access Anti-Virus scan exclusions

To reduce the load on the SharePoint server caused by on-access Anti-Virus scanning, you can specify file formats or file name masks to be excluded from scanning and set the maximum size of files to scan.

► *To exclude unwanted file formats from on-access anti-virus scanning:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **On-access scan** node.
2. In the workspace, select the **Exclusions from scan** tab.
3. In the **File formats** list, select the check boxes next to the items in the file formats tree that correspond to the relevant formats.

   Make a convenient use of the tree with the **Expand all** and **Minimize all** buttons.
4. To save the changes, click the **Save** button.

► *To exclude files that match specific masks from Anti-Virus scanning:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **On-access scan** node.
2. In the workspace, select the **Exclusions from scan** tab.
3. In the **File masks** list, select the check boxes next to file name masks to be excluded from the scan scope.
4. To add a mask to the list, open the **Adding file mask** window by clicking the **Add** button, and specify the mask in the entry field. To save the mask and close the window, click **OK**. The mask will be displayed in the **File masks** field.

   If you want to set multiple masks, use semicolon to separate them in the entry field (see the section "File name mask creation rules" on page 111).
5. To save the changes, click the **Save** button.

Configuring object processing rules for on-access scanning

Kaspersky Security will handle infected, probably infected, corrupted and password-protected files depending on the values of Anti-Virus scan settings of the SharePoint server (see section "Kaspersky Security operation depending upon the SharePoint server settings" on page 82).

► *To create object processing rules for anti-virus scanning:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **On-access scan** node and click the **General** tab in the workspace.
2. In the **Anti-Virus scan** section, open the **Actions with infected and probably infected files** dropdown list and select one of the following actions:
   - **Disinfect**. Kaspersky Security attempts to disinfect the file. If the file cannot be disinfected, Kaspersky Security blocks it (the file is not uploaded to the SharePoint server or downloaded from the server to the user's computer).
   - **Block**. Kaspersky Security blocks the file.
   - **Skip**. Kaspersky Security does not perform any action on the file. The file can be uploaded to the SharePoint server or downloaded from the server to the user computer.
3. In the **Anti-Virus scan** section, open the **Actions with password-protected files** dropdown list and select one of the following actions:
   - **Disinfect**. Kaspersky Security blocks the file. The file cannot be uploaded to the SharePoint server or downloaded from the server to the user computer.
   - **Skip**. Kaspersky Security does not perform any action on the file. The file can be uploaded to the SharePoint server or downloaded from the server to the user computer.
4. In the **Anti-Virus scan** section, open the **Actions with corrupted files** dropdown list and select one of the following actions:
   - **Block**. Kaspersky Security blocks the file. The file cannot be uploaded to the SharePoint server or downloaded from the server to the user computer.
   - **Skip**. Kaspersky Security does not perform any action on the file. The file can be uploaded to the SharePoint server or downloaded from the server to the user computer.

   > If the **Skip** option is selected, Kaspersky Security does not take any action on the file, but the file is assigned one of the status labels based on the scan results (see the section "About on-access scan" on page 79). Information about the file will be recorded in reports (see page 146) and statistics (see page 76).

5. To save the changes, click the **Save** button.

► *To create object processing rules for content filtering:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **On-access scan** node and click the **General** tab in the workspace.
2. In the **Content filtering** section, open the **Actions with files that contain unwanted content** dropdown list and select one of the following actions:
   - **Block**. Kaspersky Security blocks the file. The file cannot be uploaded to the SharePoint server or downloaded from the server to the user computer.
   - **Skip**. Kaspersky Security does not perform any action on the file. The file can be uploaded to the SharePoint server or downloaded from the server to the user computer.
3. To save the changes, click the **Save** button.

> If the **Skip** option is selected, Kaspersky Security does not take any action on the file, but the file is assigned one of the status labels based on the scan results (see the section "About on-access scan" on page 79). Information about the file will be added to reports and statistics.

Configuring additional settings for on-access content filtering

You can configure additional settings for on-access Content filtering: specify prohibited file formats, masks of unwanted file names, unwanted words or phrases.

► *To specify prohibited file formats:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **On-access scan** node.
2. In the workspace, select the **Content Filtering rules** tab.
3. In the **Unwanted file formats** list, select the check boxes next to unwanted file formats.

   Make a convenient use of the tree with the **Expand all** and **Minimize all** buttons.
4. To save the changes, click the **Save** button.

► *To specify the masks for unwanted file names:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **On-access scan** node.
2. In the workspace, select the **Content Filtering rules** tab.
3. In the **Unwanted file names** list, select the check boxes next to unwanted file name masks.

   > In the **Content filtering** node you can add and edit the sets of unwanted file name masks using the **Filter by masks** tab.

4. To save the changes, click the **Save** button.

► *To define unwanted words and phrases:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **On-access scan** node.
2. In the workspace, select the **Content Filtering rules** tab.
3. In the **List of categories** list, select the check boxes next to categories of unwanted words and phrases.

   > You can add and edit custom categories of unwanted words and expressions in the **Content filtering** node using the tab **Filter by keywords**.

4. To save the changes, click the **Save** button.

Enabling and disabling on-access anti-virus scanning

► *To enable or disable anti-virus scanning:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **On-access scan** node.
2. On the **General** tab, perform one of the following actions:
   - Select the **Enable Anti-Virus scan** check box if you want the application to perform on-access anti-virus scanning of the file.

- Clear the **Enable Anti-Virus scan** check box if you do not want the application to perform on-access anti-virus scanning of the file.

3. Click the **Save** button.

Enabling and disabling on-access content filtering

► *To enable or disable Content Filtering:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **On-access scan** node.
2. On the **General** tab, perform one of the following actions:
   - Select the **Enable Content filtering** check box if you want the application to perform content filtering of the file during on-access scanning.
   - Clear the **Enable Content filtering** check box if you do not want the application to perform content filtering of the file during on-access scanning.
3. Click the **Save** button.

> For Content filtering to work properly, the Kaspersky Security account must have site collection administrator privileges (for all site collections) and administrator privileges for the SQL database containing the site collection.

Enabling and disabling SharePoint web object scanning

► *To enable or disable the scanning SharePoint web objects:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **On-access scan** node.
2. On the **General** tab, perform one of the following actions:
   - Select the **Scan SharePoint web content** check box if you want the application to scan SharePoint web objects when they are created or modified.

- Clear the **Scan SharePoint web content** check box if you do not want the application to scan SharePoint web objects when they are created or modified.

> Kaspersky Security scans SharePoint web objects if Content Filtering is enabled (the **Enable Content filtering** check box is selected).

If the **Scan SharePoint web content** check box is selected, the application scans created or modified SharePoint web objects for unwanted words or phrases included in Kaspersky Lab sections and user categories within the search scope configured in the settings of content Filtering (see the section "Configuring additional settings for on-access content filtering" on page 87).

On detecting unwanted content in a SharePoint web object, the application makes a corresponding record in the application log and the Windows event log. Kaspersky Security does not save the SharePoint web objects or move them to Backup. The application shows a message that such SharePoint web object cannot be saved or modified.

> If Kaspersky Security blocks a SharePoint web object under Microsoft SharePoint Server 2010, the application may fail to save the changes made to this SharePoint web object or the newly created SharePoint web object.

3. Click the **Save** button.

Enabling and disabling Anti-Phishing scanning of web content

► *To enable or disable Anti-Phishing scanning of web content:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **On-access scan** node.
2. On the **General** tab in the **Content filtering** section, perform one of the following actions:
   - Select the **Scan content of SharePoint web objects for phishing** check box if you want the application to scan the content of a created or modified SharePoint web object for links appearing on the lists of malicious or phishing URLs.

- Clear the **Scan content of SharePoint web objects for phishing** check box if you do not want the application to scan the content of a created or modified SharePoint web object for links appearing on the lists of malicious or phishing URLs.

  Kaspersky Security scans web content for malicious and phishing links if Content Filtering is enabled (the **Enable Content filtering** check box is selected) and scanning of SharePoint web objects is enabled (the **Scan SharePoint web content** check box is selected).

  If the **Scan content of SharePoint web objects for phishing** check box is selected, the application checks URLs against the Kaspersky Lab database of malicious and phishing URLs when web content is created or modified. If Kaspersky Security Network is used to protect a server or servers, information about the malicious or phishing URL can be relayed to the KSN service (see section "KSN Protection Settings" on page 116)).

  On detecting a phishing threat in a SharePoint web part, the application logs information about it in Reports (see page 146).

3. Click the **Save** button.

On-demand scan

This section provides information about on-demand scanning as a way of scanning files and web objects that the application has not scanned in real-time mode. The section describes the operating mechanism of on-demand scanning and provides instructions on how to define the scan settings.

In this section

About on-demand scan

On-demand scan is scanning of files on a SharePoint server, which is performed manually or according to a schedule created in advance.

Kaspersky Security performs on-demand scan on:

- files located on the SharePoint server and in areas of the SharePoint structure specified in the scan settings;
- all SharePoint web objects (such as wiki pages and forums hosted on the SharePoint server);
- SharePoint service files.

The application scans only the last versions of files and SharePoint web objects hosted on the SharePoint server.

During on-demand scanning, Kaspersky Security performs:

1. Anti-virus file scanning in accordance with the scan exclusions settings (see section "Creating on-demand anti-virus scan exclusions" on page 100).
2. Scans files for fragments of malicious code typical of exploits;
3. Scanning for unwanted file formats and unwanted file names (see section "Configuring additional settings for on-access Content filtering" on page 87);
4. Scanning of files and SharePoint web objects for unwanted content (see section "Configuring additional settings for on-access Content filtering" on page 87).

If a file has been blocked by Content filtering, the application does not perform Anti-Virus scanning of this file. Alternatively, if a file has been blocked following an Anti-Virus scan, the application does not apply Content filtering to the file.

Status labels assigned to files based on scan results

Based on the results of Anti-Virus scanning, Kaspersky Security assigns one of the following status labels to the file:

- *Not infected*. No threats detected in the file.
- *Infected*. A file a segment of whose code fully matches a code segment of a known threat.
- *Probably infected*. A file whose code contains a modified segment of code of a known threat, or a file resembling a threat in the way it behaves.
- *Password-protected*. A password-protected archive.
- *Corrupted.* The file cannot be read by Kaspersky Security.

Based on the results of content filtering, Kaspersky Anti-Virus assigns one of the following status labels to the file:

- *Allowed.* There is no unwanted content in the file.
- *Forbidden format*. The file has an unwanted format.
- *Forbidden mask*. The file name contains an unwanted mask.
- *Forbidden content*. The file has been found to contain unwanted words and phrases.

Based on the results of content filtering, the application assigns one of the following status labels to the SharePoint web part:

- *Allowed.* The SharePoint web object does not contain unwanted content.
- *Forbidden content*. The SharePoint web object has been found to contain unwanted content.

On-demand scan tasks

To run an on-demand scan in Kaspersky Security, create an on-demand scan task or tasks (see section "Creating an on-demand scan task" on page 95). You can configure anti-virus scanning and content filtering settings for each on-demand scan task, and define a schedule.

On-demand scan tasks can be run manually or scheduled to run automatically. After performing each scan task, the application generates a report (see section "Viewing an on-demand scan task report" on page 102).

The list of on-demand scan tasks is displayed in a table in the workspace of the **On-demand scan** node. The on-demand scan tasks that were not run or could not be run at the scheduled time are highlighted in red. Color highlighting is not used for other tasks.

The reasons for not running the tasks are displayed in the **Status** column:

- **Task server does not exist**. Kaspersky Security Server has been deleted from the SharePoint server specified in the on-demand scan task settings. You can specify a different SharePoint server in the task settings.
- **Task not executed**. The SharePoint server specified in the on-demand scan task settings was not available at the time scheduled for the start of the task. The availability of the SharePoint server needs to be checked. You can run a task manually, if necessary.

Creating an on-demand scan task

► *To create an on-demand scan task:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **On-demand scan** node.
2. Click the **Create** button in the workspace.

   This opens the **Task settings** window.
3. In the **Task name** field, enter the name of the task.
4. Configure restrictions for the newly created on-demand scan task:
   - If you want Kaspersky Security to move copies of files to Backup before processing, select the **Move files to backup** check box.
   - If you want to limit the duration of an on-demand scan task, select the **Restrict the duration of task execution** check box and specify a value in the field on the right.
   - If you want the application to scan SharePoint service files while performing the task, select the **Scan service files** check box.
   - If you want to limit the duration for a scan of each individual file, select the **Scan timeout** check box and enter a value (in seconds) in the field on the right.
   - If you want to run the task on a different SharePoint server, select the relevant SharePoint server in the **Run task on server** dropdown list.
5. In the **Schedule** section, set up a schedule for the on-demand scan task:
   - If you want to run the on-demand scan task manually at your convenience, select **manually**.
   - If you want the on-demand scan task to run once at the specified time, select **Once** and specify the date and time for task start.
   - If you want the on-demand scan task to run automatically every week, select **Weekly** and specify the days and time for task start.

     > If the **Once** or **Weekly** option is selected, the application uses the time set on the SharePoint server where the task will be run.

6. If necessary, in the **Anti-Virus scan** section, select the **Enable Anti-Virus scan** check box and configure actions to be performed by the application on infected, potentially infected, password-protected, and corrupted files during the task run:

    a. In the **Actions with infected and probably infected files** dropdown list, select an action:

    - **Disinfect**. Kaspersky Security attempts to disinfect an infected or probably infected file. If the file cannot be disinfected, the application replaces it with a text file describing the reason for deletion.
    - **Delete**. Kaspersky Security replaces the infected or probably infected file with a text file describing the reason for deletion.
    - **Skip**. Kaspersky Security does not perform any operations on the infected or potentially infected file.

    > After an infected file is deleted, Kaspersky Security also deletes all of its versions (regardless of whether they have been infected). We recommend that you save your files in Backup in order to avoid data losses.

    b. In the **Actions with password-protected files** dropdown list, select an action:

    - **Delete**. Kaspersky Security replaces the password-protected file with a text file describing the reason for deletion.
    - **Skip**. Kaspersky Security does not perform any action on the password-protected file.

    c. In the **Actions with corrupted files** dropdown list, select an action:

    - **Delete**. Kaspersky Security replaces a corrupted file with a text file describing the reason for deletion of the original file.
    - **Skip**. Kaspersky Security does not perform any action on the corrupted file.

    > If the **Skip** option is selected, the application does not take any action on the file, but assigns one of the status labels to the file based on the scan results (see the section "About on-demand scanning" on page 92). The application records the file details in reports and statistics.

7. If necessary, select the **Enable Content filtering** check box and set the action to be performed on files with unwanted content by selecting one from the **Actions with files that contain unwanted content** dropdown list:

    - **Delete**. Kaspersky Security replaces a file with unwanted content with a text file describing the reason for deletion of the original file.

      > If Kaspersky Security detects unwanted content in a SharePoint service file, it does not delete this file. The application records information about unwanted content in the SharePoint service file in the task report and the application log.

    - **Skip**. Kaspersky Security does not perform any action on the file containing unwanted content.

      > If the **ContentFiltering_ProtectionAction_Skip** option is selected, the application does not take any action on the file, but assigns one of the status labels to the file based on the scan results (see section "About on-demand scanning" on page 92). The application records the file details in reports and statistics.

8. If you want the application to scan SharePoint web objects (such as wiki pages and forums hosted on a SharePoint server) with Content Filtering, select the **Scan SharePoint web content** check box.

    If the **Scan SharePoint web content** check box is selected, the application scans SharePoint web objects for unwanted words or phrases included in Kaspersky Lab sections and custom categories whose settings are configured in the **Content filtering** node.

    If the application detects unwanted content in a SharePoint web part, it records information about this in the on-demand scan report (see section "Viewing an on-demand scan task report" on page 102) and the application log. Kaspersky Security does not delete the SharePoint web object or move it to Backup.

    > For Content filtering to work properly, the Kaspersky Security account must have site collection administrator privileges (for all site collections) and administrator privileges for the SQL database containing the site collection.

9. Click the **OK** button.

    The task that has been created will be added to the list of tasks in the workspace of the **On-demand scan** node.

You can configure additional settings for an on-demand scan task:

- Select or exclude areas of the SharePoint structure from the scan scope (see section "Selecting and excluding from on-demand scanning areas of the SharePoint structure" on page 98).
- Exclude certain file types, file formats, or file name masks from the anti-virus scan, restrict file scan duration, and disable scanning of archives (see section "Creating on-demand Anti-Virus scan exclusions" on page 100);
- Configure content filtering (see section "Configuring Content filtering" on page 101).

Selecting and excluding from on-demand scanning areas of the SharePoint structure

You can specify areas of the SharePoint structure to be scanned during an on-demand scan task. You can also exclude individual areas of the SharePoint structure from scanning.

► *To define the scan scope in a SharePoint structure:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **On-demand scan** node.
2. In the list of tasks displayed in the workspace, select the on-demand scan task that you want to modify. Click the **Change** button to open the **Task settings** window on the **Scan scope** tab.
3. Specify the scan scope in the SharePoint structure in one of the following ways:
   - In the SharePoint server structure tree, select check boxes corresponding to the SharePoint structure areas that you want to include in the scan scope. All check boxes are selected by default (all available SharePoint structure areas are scanned during the on-demand scan task).

     > The tree only displays the SharePoint structure areas, for which administrator access is allowed to the account used to start the application services.

- Add SharePoint structure areas manually. To do this, in the **Additional web addresses** section, perform the following actions:

   a. Click the **Add** button. In the window that opens, enter the path to the area that you want to add and click **OK**.

   The following types of paths are supported:

   - `http://<SharePoint portal name>.local/content/`;
   - `https://<SharePoint portal name>.local:8080/content/file.txt`;
   - `http://<SharePoint portal name>/`.

   To remove an area, select one in the list and click the **Delete** button.

   b. Select the check box opposite the path to a SharePoint structure area, and select **Include** in the drop-down list.

   c. Clear the check box opposite the path to a SharePoint structure area, and select **Exclude** in the drop-down list.

4. Click **OK** to save the changes and close the window.

► *To exclude SharePoint structure areas from an on-demand scan:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **On-demand scan** node.

2. In the list of tasks displayed in the workspace, select the on-demand scan task that you want to modify. Click the **Change** button to open the **Task settings** window on the **Scan scope** tab.

3. Exclude a SharePoint structure area from scanning in one of the following ways:

   - In the SharePoint server structure tree, clear the check boxes corresponding to the areas which you want to exclude from the scan scope.

   - In the **Additional web addresses** section, select the **Exclude** action in the dropdown lists for the areas that you want to exclude from scanning.

4. Click **OK** to save the changes and close the window.

Creating on-demand Anti-Virus scan exclusions

To ease the load on the SharePoint server, you can exclude files from the scope of on-demand Anti-Virus scanning specific formats or file name masks, restrict scanning duration for individual files, as well as disable scanning of archives.

► *To exclude specific file formats from on-demand anti-virus scanning:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **On-demand scan** node.
2. In the list of tasks displayed in the workspace, select the on-demand scan task that you want to modify. Click the **Change** button to open the **Task settings** window, then select the **Exclusions from scan** tab.
3. In the **File formats** list, select the check boxes next to the file formats that you want to exclude from scanning.

   Make a convenient use of the tree with the **Expand all** and **Minimize all** buttons.
4. To save the changes and close the window, click **OK**.

► *To exclude files that match specific masks from on-demand Anti-Virus scanning:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **On-demand scan** node.
2. In the list of tasks displayed in the workspace, select the on-demand scan task that you want to modify. Click the **Change** button to open the **Task settings** window and select the **File formats** tab.
3. In the **File masks** list, select the check boxes next to file name masks to be excluded from the scan scope.
4. To add a mask to the list, open the **Adding file mask** window by clicking the **Add** button, and enter the mask in the entry field (see the section "File name mask creation rules" on page 111).

   If you want to define several masks at once, use a semicolon as a separator.
5. To save the changes and close the window, click **OK**.

Configuring content filtering

For on-demand scan tasks, you can configure the application to look for specific file formats, file name masks, and the categories of unwanted words and phrases.

► *To configure Content filtering in an on-demand scan task:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the node **On-demand scan**.

2. In the list of tasks displayed in the workspace, select the on-demand scan task that you want to modify. Click **Change** to open the **Task settings** window and select the **Content filtering rules** tab.

3. Configure the following Content filtering settings:

   - In the **List of categories**, select the check boxes next to the categories of Kaspersky Lab and user categories, which the application should seek while running the on-demand scan task.

   - In the **Unwanted file formats** list, select check boxes next to the file formats that should be scanned. To expand / collapse the entire list of formats and extensions, use the **Expand all** and **Collapse all** button.

   - In the **Sets of unwanted file name masks** list, select check boxes next to the sets of file name masks to be scanned during on-demand scanning.

4. To save the changes and close the window, click **OK**.

> You can specify the file formats and file name masks and the set of categories of unwanted words and phrases in the **Content filtering** node.

Starting and stopping on-demand scan tasks

► *To start an on-demand scan task:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **On-demand scan** node.
2. Select an on-demand scan task from the list in the workspace.
3. Click the **Start** button to run the on-demand scan task, or click the **Stop** button to stop the task.

Viewing an on-demand scan task report

► *To view a report on the results of an on-demand scan task:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **On-demand scan** node.
2. Select a task from the list in the workspace.
3. Click the **Report** button.

   The report is displayed in a new window of your web browser.

   > The **Report** button is not available for tasks currently in progress and for tasks that have never been started.

The report contains the following information on the last on-demand scan:

- **Used task settings**:
  - task name;
  - task launch method (manual or scheduled);
  - scan task start and end times;

  - information about enabled application components;
  - name of the SharePoint where the task was performed;
  - task status;
- **Scan results**. Summarized information about the results of the on-demand scan task.
  - **Processing errors**. The number of files skipped by the application because of scanning errors.
  - **Scanned items**. Total number of scanned files.
  - **Virus threats found**. The number of malicious objects detected (the number Anti-Virus component incidents).
  - **SharePoint web objects scan alarms**. Number of detected files in an unwanted format and file names containing unwanted masks, as well as web objects with unwanted content (number of Content filtering incidents).
- **Table of positives**. A table with information about all files found to contain malicious objects or violations of Content filtering rules. If the scan has not detected any virus threats or violations of content filtering rules, the *File scan detected no incidents* message is displayed instead of the table of positives.
  - **File name**. The name and path to the file where malicious objects or violations of content filtering rules have been found.
  - **Version**. File version on the SharePoint server.
  - **Action**. Operation performed on the file based on the scan results in accordance with the defined settings.
  - **Anti-Virus scan**. Status assigned to the file by the anti-virus scanning component. This column shows the *Corrupted* or *Password protected* status label for corrupted or password-protected files. This column shows the name of the object detected in the file for infected or probably infected files.
  - **Content filtering**. Status assigned to the file by the content filtering. Policies whose violation triggered the content filtering component.

  - **Backup**. Information about creation of a backup copy for the file in Backup.
  - **Restored version**. The version to be assigned to the restored file (if it can be disinfected).
  - **Incident ID**. The universal ID of the positive. The incident ID simplifies the search for information about the incident in the report, Backup, and file log. It is also displayed in the properties of a backup copy of the file in Backup and in notifications about violations of security policies during on-demand scanning.

- **SharePoint web objects scan alarms**. A table with the details of SharePoint web objects found to contain unwanted words or phrases. If no unwanted words or phrases have been detected during a scan of SharePoint web objects, the *SharePoint web objects scan detected no incidents* message is displayed instead of this table.
  - **Name and version**. Name and version of a SharePoint web object found to contain unwanted words or phrases included in Kaspersky Lab sections and user categories within the search scope configured in the Content filtering settings. The name consists of: `<Site name> / <List name> / <Object ID>`. The field contains `n/a` if the version information of the scanned SharePoint web object is unavailable.
  - **Categorized as**. List of SharePoint web object fields found to contain unwanted words or phrases, and categories to which the detected words and phrases belong.
  - **Incident ID**. The universal ID of the positive. The incident ID simplifies the search for information about the incident in the report and log file.

- **Table of locations to scan**. The list of all scan areas specified in the on-demand scan task settings.

Deleting an on-demand scan task

► *To delete an on-demand scan task:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **On-demand scan** node.
2. In the workspace, select the task that you want to remove and click the **Delete** button.

Scanning of SharePoint content

This section contains information about Content filtering and how to configure it.

In this section

About Content filtering

Kaspersky Security performs content filtering of files placed on the SharePoint server during on-access scanning (see section "On-access scan" on page 79) and on-demand scanning (see section "On-demand scan" on page 92).

Content is filtered by:

- file format
- file name mask You can specify masks for unwanted file names and formats.
- By the text content and names of the files. Kaspersky Security includes a preset collection of categories of unwanted words and phrases created by the experts at Kaspersky Lab. The preset collection of unwanted words and phrases cannot be modified nor updated. The window for adding new user categories of words and phrases.

File content is scanned using the libraries of filters via the IPersistStream interface. To enable or disable filters available on a server, you can use IFilter utility, which is installed along with Kaspersky Security.

> More details about IFilter can be found at http://msdn.microsoft.com/en-us/library/ms691105%28v=vs.85%29.aspx.

When the application is installed, filters included in following standard filter packs are enabled by default:

- Windows Server (installed with the operating system).
- SharePoint (installed with the SharePoint server).
- Office 2007 Filter Pack
- Office 2010 Filter Pack

If other filters are installed on the SharePoint server, they are disabled by default and content filtering by format is not performed for files scanned using these filters. Use Kaspersky IFilter Utility to enable such filters.

You can enable / disable the installed filters and also install necessary additional filters using utility.

You can start the utility from the menu **Start** → **Programs** → **Kaspersky Security 9.0 for SharePoint Server** → **Kaspersky IFilter Utility**.

For more details on the Kaspersky IFilter Utility, please refer to the online Help file.

Creating, renaming, and deleting user categories of unwanted words and phrases

► *To create a new user category of unwanted words and phrases:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Content filtering** node.
2. In the workspace, select the **Filter by keywords** tab and click the **Create** button in the **List of categories** section.

3. In the **Category name** window that opens, enter a name for the new category.

4. Click the **OK** button.

► *To rename a user category of unwanted words and phrases:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Content filtering** node.

2. In the workspace, click the **Filter by keywords** tab, select the category that you want to rename, and click the **Rename** button.

3. In the **Category name** window that opens, enter the name of the category and click **OK**.

► *To delete a category for unwanted words and phrases:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Content filtering** node.

2. In the workspace, click the **Filter by keywords** tab, in the **List of categories** section, select the category that you want to delete, and click the **Delete** button. Selected category will be removed from the list.

> Only user categories can be created, renamed or deleted. You cannot change the preset collection of Kaspersky Lab categories included in the application.

Adding, changing, and deleting unwanted words and phrases in user categories

► *To add an unwanted word or phrase to a user category:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Content filtering** node.

2. In the workspace, click the **Filter by keywords** tab, and in the **List of categories** field, select the custom category to which you want to add a word or phrase.

3. In the **Category structure** field, click the **Add** button. Type the word or phrase in the field within the displayed dialog.

4. If you want the application to consider case while searching for a word or phrase, select the **Case-sensitive** check box.

5. Click the **OK** button.

> You can specify several words or phrases. Use the "|" character as a delimiter.

► *To edit a word or phrase within a selected user category:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Content filtering** node.

2. In the workspace, click the **Filter by keywords** tab, and in the **List of categories** field, select the custom category containing the word or phrase that you want to edit.

3. In the **Category structure** field, select the word or phrase that you want to edit, and click the **Change** button.

4. Edit the word or phrase in the displayed window. If necessary, select the **Case-sensitive** to enable case sensitivity.

5. Click the **OK** button.

► *To delete a word or phrase from a selected user category:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Content filtering** node.

2. In the workspace, select the **Filter by keywords** tab, and in the **List of categories** field, select the custom category containing the word or phrase that you want to delete.

> You can select several words of phrases in the list while holding the **SHIFT** key pressed.

3. In the **Category structure** field, select the word or phrase that you want to delete, and click the **Delete** button.

> Only user categories can be created, edited or deleted. You cannot change the preset collection of Kaspersky Lab categories included in the application.

Importing a list of unwanted words and phrases into a user category from a text file

You can import from a text file a list of unwanted words and phrases into a user category.

The words and phrases in such file must comply with the following conditions:

- Each line must contain just one term with its word forms.
- The term should be separated from its word forms with the "|" character.
- Term length may not exceed 127 characters.

> If a term contains special symbols or multibyte characters, for example, UTF-8 (encoded using three or more bytes), the term length must not exceed 64 characters.

► *To import a list of unwanted words and phrases into a user category:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Content filtering** node.
2. In the workspace, select the **Filter by keywords** tab, and in the **List of categories** field, select the category to which you want to import the list.
3. In the **List of categories** field, click the **Import from file** button. In the displayed window specify the path to the necessary file.

   > The **Import from file** button is only available for custom categories of unwanted words and phrases.

4. To save the changes, click the **Save** button.

About the white list

The while list is a list of words and / or phrases that should be skipped by Content filtering.

The white list contains words and / or phrases that, although included in prohibited categories of Kaspersky Lab, should be ignored by Content Filtering. By using the white list, it is possible to avoid false positives of the application component on detecting words and / or phrases that are permissible in and specific to the field of the company's business.

The white list is local. It is created separately for each farm server (see section "Creating the white list" on page 110). When a word and / or phrase is included in the white list, all of its word forms should be specified for the application component to work properly.

Example:

<string>sea</string>

<string>seas</string>

<string>seaside</string>

<string>seasick</string>

Changes made to the list are applied with a delay of no more than 5 seconds.

Creating the white list

► *To create a white list of permissible words and / or phrases:*

1. Open the folder with SharePoint server configuration files by performing the following:

   - If the application is installed on a farm of SharePoint servers, open the application setup folder and go to the folder of the corresponding farm server. Then open the **Configurations** folder.

   - If the application is installed on a standalone SharePoint server, open the application setup folder and go to the **Configuration** folder.

2. Create an XML file with the name ContentFilteringWhitelist.

   The ContentFilteringWhitelist.config file must have the following structure:

   ```
   <?xml version="1.0" encoding="utf-16"?>

   <configuration version="1.0">

   <ContentFilteringWhitelistSubset Contentxmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xmlns:xsd="http://www.w3.org/2001/XMLSchema">

   <Items>

   <string></string>

   </Items>

   </ContentFilteringWhitelistSubset>

   </configuration>
   ```

3. Type the word or phrase to be skipped by Content filtering between the <string> and </string> tags.

   Type each new word or phrase and their word forms in a new line between the <string> and </string> tags.

4. Save changes to the file in Unicode format.

> If you save the file in a different format, the words and / or phrases typed using a Cyrillic font may be displayed incorrectly in the error log.

File name mask creation rules

Please follow these guidelines on creating masks:

- The following wildcards are supported:
  - * – an arbitrary string of characters. For example, the "abc*" mask stands for any file with the name beginning with the "abc" string: abc.exe, abc1.com, abc2.rar.

    - ? – any single character. For example, the "abc?.exe" mask stands for any file with the name beginning with the "abc" string followed with an arbitrary single character, like abc1.exe. However, the file abc12345.exe will not match the mask.

- Observe the following restrictions:

    - Masks cannot contain the following characters: >, <, \, /, |, ", ;.

    - It is not recommended to use masks that match the file extensions of SharePoint service files (for example, *.aspx, *.html, *.mht) in the content filtering settings. Deleting SharePoint service files could disrupt the operation of SharePoint.

Creating, renaming, and deleting a set of masks for unwanted file names

► *To create a new set of forbidden file name masks:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Content filtering** node.

2. In the workspace, on the **Filter by masks** tab, click the **Add** button. This opens the **Set name** window.

3. Enter in the displayed dialog the name for the new set of masks.

4. Click the **OK** button.

► *To rename a set of masks for unwanted file names:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Content filtering** node.

2. In the workspace, on the **Filter by masks** tab, select the set of masks that you want to rename, and click the **Rename** button.

3. Enter the new name for the set of masks in the window that opens, and click **OK**.

► *To delete a set of unwanted file name masks:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Content filtering** node.
2. In the workspace, on the **Filter by masks** tab, select the set of masks that you want to delete, and click the **Delete** button.

Changing a set of unwanted file name masks

► *To add an unwanted file name mask to a set:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Content filtering** node.
2. In the workspace, select the **Filter by masks** tab, and in the **Mask sets** field, select the set to which you want to add a mask.
3. In the **Masks in set** field, click the **Add** button. In the window that opens, specify the mask of the unwanted file name in the field.

> You can specify several masks. Use a semicolon as a delimiter.

► *To edit the unwanted file name masks in a set:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Content filtering** node.
2. In the workspace, click the **Filter by masks** tab, and in the **Mask sets** field, select the set in which you want to edit masks.
3. In the **Masks in set** field, select the mask that you want to edit, and click the **Edit** button.
4. In the window that opens, edit the mask and click **OK**.

► *To delete an unwanted file name mask from a set:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Content filtering** node.
2. In the workspace, click the **Filter by masks** tab, and in the **Mask sets** field, select the set from which you want to delete masks.

   > You can select several masks in the set while holding the **SHIFT** key pressed.

3. In the **Masks in set** field, select the mask that you want to delete, and click the **Delete** button.

   > If multiple masks have been selected within a set, you can only delete the selected masks. No other operations with them will be available.

Configuring the application settings

This section describes configuration of the following application settings:

- Email message delivery settings
- Logging settings
- Backup purging settings

In this section

About participation in Kaspersky Security Network

To protect SharePoint servers more effectively, Kaspersky Security uses data that is collected from users around the globe. *Kaspersky Security Network* is designed to process such data.

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

Your participation in Kaspersky Security Network helps Kaspersky Lab to gather real-time information about the types and sources of new threats, develop methods of neutralizing them, and reduce the number of false alarms. Participation in Kaspersky Security Network also lets you access reputation statistics for applications and websites.

When you participate in Kaspersky Security Network, certain statistics are collected while Kaspersky Security is running and are automatically sent to Kaspersky Lab. This information makes it possible to keep track of threats in real time. 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.

> Participation in Kaspersky Security Network is voluntary. To start using Kaspersky Security Network, you have to accept the terms of a special agreement – the Kaspersky Security Network Statement (see section "KSN Protection Settings" on page 116). You can also opt out of participating in Kaspersky Security Network at any time (see the section "KSN Protection Settings" on page 116). No personal data of the user is collected, processed, or stored by the Kaspersky Security Network services. The types of data that Kaspersky Security sends to Kaspersky Security Network are also described in the Kaspersky Security Network Statement. You can use Kaspersky Security Network services if the application license has not yet expired and the key has not been blacklisted.

KSN Protection Settings

► *To configure the KSN protection settings:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Settings** node.
2. In the **Use of Kaspersky Security Network** section, select the **I have read the KSN Statement and accept all of the conditions therein** check box if you accept all of the conditions of the Kaspersky Security Network Statement. You can view its text by clicking the **KSN Participation Agreement** button.
3. To use KSN cloud services for protection of SharePoint web objects, select the **Use Kaspersky Security Network** check box.

   Information received from Kaspersky Security Network services is used during anti-virus scans and scans of web objects for phishing threats.

4. Set the **Maximum waiting time when requesting KSN**. The default wait time for a response from the cloud is 10 seconds.

5. Select the **Use proxy server to access KSN** check box if you want to exchange information with KSN services using a proxy server.

   The way to configure the proxy server settings is described in the automatic database update configuration instructions (see page 124).

6. Click the **Save** button.

Enabling and disabling Data Leak Prevention

The DLP (Data Leak Prevention) Module is a Kaspersky Security component designed to protect data against leaks. The component monitors file uploads by users to SharePoint in real time, checking the file contents for any confidential data. Settings of the DLP Module are configured by the Security Officer.

The **Data Leak Prevention** section is displayed in the **Settings** node if the DLP Module component has been installed on the SharePoint server. Data Leak Prevention is enabled by default.

> Disabling the DLP Module can affect the workflow of the Security Officer.

► *To enable or disable DLP functionality:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Settings** node.

2. In the **Data Leak Prevention** section, perform one of the following actions:

   - Select the **Enable DLP Module** check box if you want the application to monitor data leaks in real-time mode.

   - Clear the **Enable DLP Module** check box if you do not want the application to monitor data leaks in real-time mode.

3. If necessary, in the **Allow running search tasks on the following servers** list, select the check boxes next to servers on which the security officer will be able to run scan tasks to search SharePoint servers for confidential data.

   > During a search task, the load on SharePoint servers increases.

4. To keep the changes, click the **Save** button in the upper part of the window.

Information about changes in the component operation is displayed in the Control Center node and in the root node of the Security Officer.

Configuring the path to the logs folder

► *To configure the path to the logs folder:*

1. In the Administration Console tree, select and open the node that corresponds to the relevant SharePoint server, then select the **Settings** node.

2. In the **Diagnostics** section, in the **Logs folder** entry field, specify the path to the logs folder.

   > Avoid using variables and masks when specifying the path to the folder. Do not specify an FTP server or a network folder as a location where the application logs are stored.

   The application will save logs using the specified path. If you configure the path to the folder on a server within a farm, the configuration will cover the entire server farm.

3. If necessary, click the **Default** link to restore the default path to the logs folder.

4. Click the **Save** button in the upper part of the window.

If the application does not save logs using the specified path, check the rights of access to that folder.

Configuring the log storage term

► *To configure the storage term for log files:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Settings** node.
2. In the **Diagnostics** section, in the **Log storage period** field, specify a value for the log storage term (in days).

   The application will store logs during the specified number of days since the last record is added to the log. If no new records have been added to a log over the specified time period, the application deletes the log.
3. Click the **Save** button in the upper part of the window.

Configuring the detail level of event logs

► *To configure the detail level of event logs:*

1. In the Administration Console tree, select and open the node that corresponds to the relevant SharePoint server, then select the **Settings** node.
2. Click the **Settings** button in the **Log details** section.

   This opens the **Diagnostics settings** window.
3. Select events that must be recorded in detail.
4. Click **OK** 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 record main events in the application 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 changes to **Maximum**. The application will record detailed information about all events to logs.

   > When maintaining a log with the advanced detail level, this log contains web addresses that have been scanned for phishing.

5. If you want to reset the current detail level of a log, click the **Reset** button.

   The application changes the detail level to **Minimum**. Logs will only contain basic events from the application operation, such as scan results, updates of databases, and keys added.

6. If necessary, select the **Record details of events to Content Filtering log** check box.

   The application will record to the Content Filtering log a text fragment that is related to a content filtering event.

7. Click the **Save** button in the upper part of the window.

Configuring automatic backup clearing

► *To configure automatic Backup purging:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Settings** node.

2. Select the **Clear Backup automatically if its size exceeds** check box.

3. Enter in the entry field maximum Backup size (MB).

   Supported parameter values are 1 –1048576 MB. If there is a storage size restriction and the addition of a new file exceeds this restriction, the application frees up the necessary space by deleting the oldest files. The default size of Backup is 3686 MB.

4. To save the changes, click the **Save** button in the upper part of the application window.

Failsafe support for SQL databases

Kaspersky Security supports the following failsafe technologies for SQL databases:

- Failover Clustering. Supported automatically.
- Database Mirroring. Supported automatically.
- Log Shipping. When the database used by the application (primary database) fails, the server hosting the restored database needs to be specified manually in order to switch to this database.

Using Database Mirroring technology

If your SQL server is configured to use the Database Mirroring failover support technology, the application automatically switches from the primary database that has failed to a mirror database, and then back to the primary database after it has been restored.

> If the SQL server is running in **High Performance** Mode or **High Safety Mode Without Automatic Failover** for Database Mirroring, manual switchover to Database Mirroring is required by means of the SQL server if the main database used by Kaspersky Security fails.

Using Log Shipping technology

If your SQL server is configured to use the Log Shipping failover support technology, you can switch to using a restored database when the primary database fails. This switch is performed manually.

► *To switch to the restored database when using Log Shipping technology:*

1. In the folder <Application installation folder>\Configuration, open the file BackendDatabaseConfiguration.config in a text editor.
2. Specify the name of the SQL server (indicating the SQL server instance) that hosts the failover partner in the line `<SqlServerName>SQL server name\instance</SqlServerName>`.
3. Save the file.

   The changes will take effect within one minute.

> If Kaspersky Security is installed on a SharePoint farm, the corresponding changes to the file BackendDatabaseConfiguration.config need to be made on all SharePoint farm servers.

Database update

This section describes how to configure database updates for Kaspersky Security, how to schedule automatic updates, and how to select and connect to update sources. It also includes information about how to configure each individual SharePoint server within a farm, and how to propagate global settings to all SharePoint servers in that farm.

In this section

About database updates

Kaspersky Security database updates keep SharePoint servers protected against new viruses and other threats. Databases contain the latest information about threats and ways to neutralize them.

Databases contain descriptions of all malicious programs known to date and ways of disinfecting objects that have been corrupted by malware, as well as descriptions of programs that may be used by criminals to do harm to the user's computer or data.

> While updating the databases, the application does not update the set of Kaspersky Lab categories.

It is important to keep all databases up to date. You are advised to update the databases as soon as you install the application because the databases included in the distribution kit will already be out of date. The databases on Kaspersky Lab's update servers are updated every hour.

Databases can be updated from the following sources:

- Kaspersky Lab's update servers on the Internet
- Local updates source, such as a local or a network folder
- Another HTTP or FTP server, such as your Intranet server

The updating is performed either manually or automatically, according to a schedule. After the files are copied from the specified update source, the application automatically connects to the new databases.

For added protection of SharePoint files, you can use the Kaspersky Security Network service in addition to updates of databases (see the section "About participation in Kaspersky Security Network" on page 115). These services provide up-to-date information about threats and malware before it appears in Anti-Virus and Anti-Phishing databases.

During setup on several SharePoint farm servers, you can define local update settings (see section "Configuring the local database update settings on servers of the farm" on page 126) for each individual server or propagate the global update settings (see section "Propagating global database update settings to farm servers" on page 127) to all servers.

Viewing the information about updates to the anti-virus database

► *To view the information about database updates:*

1. Select and open in the Administration Console tree the **Control Center (<Server name>)** node corresponding to the relevant SharePoint server. Then select the **Updates** node.
2. In the workspace, open the **Updates on servers** tab.

   You will see a table with information about database updates on each SharePoint farm server. The table contains the following columns:

   - **Server name**. Server within a SharePoint farm, on which Kaspersky Security is installed.
   - **Status of the last database update**. The result of the last database update.

- **Database release date (UTC)**. The time when databases currently used by the application were published on Kaspersky Lab servers.
- **Time of last database update**. The time of the latest database update on the server.
- **Settings**. Update settings used on the server (local or global).

> If Kaspersky Security is installed on a standalone SharePoint server, update-related information is displayed in the workspace of the **Update settings** section, not on the **Updates on servers** tab.

Configuring automatic database updates

► *To configure automatic database updates:*

1. Select and open in the Administration Console tree the **Control Center (<Server name>)** node corresponding to the relevant SharePoint server. Then select the **Updates** node.
2. In the workspace, click the **General** tab, and in the **Updates on servers** section, select an update source for the databases:

   - **Kaspersky Lab's servers** to download updates from Kaspersky Lab servers.
   - **HTTP server, FTP server, local or network folder** to download updates from some of the listed update sources.

     If you select this option, specify in the corresponding text box the server address, local or network folder.

   > If Kaspersky Security is installed on a standalone SharePoint server, the update source is selected in the **Updates on servers** section of the workspace, which appears on selecting the **Updates** node in the Administration Console tree.

3. The **Run mode** dropdown list allows you to set up a schedule for updates of the databases:

   - **Manually**. The update starts when you click the **Start database update on all servers** button.
   - **Periodically**. The update starts at the specified intervals.
   - **Daily**. The update starts at the specified time (the local time of the SharePoint server is used).
   - **On selected day**. The update starts on the specified days of the week.

   > If Kaspersky Security is installed on a standalone SharePoint server, the run mode for automatic updates of databases is configured in the **Database update settings** section of the workspace, not on the tab.

4. In the **Connection settings** section, specify the required connection settings:

   - If you connect to the Internet using a proxy server, select the **Use proxy server** check box and specify the proxy server address and number of the port used for connection. The default proxy server port number is 8080.
   - If the proxy server requires authentication, specify the name and password of the user account. To do this, select the **Use authentication** check box and fill in the **Account** and **Password** fields.
   - Specify the timeout duration in the **Connection timeout** entry field. By default, the timeout is set to 60 seconds.

     This proxy server is used for data exchange with the KSN cloud service when KSN protection is enabled (see the section "KSN Protection Settings" on page 116).

   > If Kaspersky Security is installed on a standalone SharePoint server, connection settings should be defined in the **Connection settings** section of the workspace displayed when you select the **Updates** node in the console tree.

5. Click the **Save** button.

Configuring the local database update settings on SharePoint servers of the farm

► *To configure the local database update settings on a SharePoint server within a farm:*

1. Select and open in the Administration Console tree the **Control Center (<Server name>)** node corresponding to the relevant SharePoint server. Then select the **Updates** node.

2. In the workspace, click the **Updates on servers** tab, select the required server in the table, and click the **Modify local settings** button.

3. In the **Server settings** window that opens, in the **General settings** section, select a source of updates:

   - **Kaspersky Lab's servers** to download updates from Kaspersky Lab servers.

   - **HTTP server, FTP server, local or network folder** to download updates from some of the listed update sources.

     If you select this option, enter the server address, local or network folder in the entry field.

4. In the **Database update settings** section, in the **Run mode** dropdown list, set up a schedule for updates of the databases:

   - **Manually**. The update starts when you click the **Start update** button.
   - **Periodically**. The update starts at the specified intervals.
   - **Daily**. The update starts at the specified time (the local time of the SharePoint server is used).
   - **On selected day**. The update starts on the specified days of the week.

5. In the **Connection settings** section, define the connection settings:

   - If you connect to the Internet via a proxy server, select the **Use proxy server** check box and specify the proxy server address and number of the port used for connection. The default proxy server port number is 8080.

- If the proxy server requires authentication, specify the name and password of the user account. To do this, select the **Use authentication** check box and fill in the **Account** and **Password** fields.
- Specify the timeout duration in the **Maximum connection timeout** entry field. By default, the timeout is set to 60 seconds.

6. Click the **Save** button.

Propagating global database update settings to SharePoint farm servers

► *To apply the global database update settings on all SharePoint servers of the farm:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Updates** node.
2. In the workspace, click the **Updates on servers** tab, select the required server in the table, and click the **Propagate global settings** button.

Notifications

This section describes notifications generated by the application, and configuration of their delivery to specified email addresses.

In this section

About notifications

Notification is an email message that contains information about an event, which occurred on a protected SharePoint Server.

Kaspersky Security supports the delivery of notifications on the following events in the application:

- Detection of infected, password-protected, and corrupted objects, or unwanted content during an on-access scan
- Detection of infected, password-protected, and corrupted objects, or unwanted content during an on-demand scan
- Change of database status and condition
- Execution of an on-demand scan task and its results
- Detection of inactive SharePoint servers
- License-related events

Kaspersky Security sends event notifications by email. The application uses a SMTP server to send notifications. You can select the SMTP server that is used on SharePoint or specify a different SMTP server (see section "SMTP server configuration for delivery of notifications" on page 131).

For each event you can specify notification recipients (see section "Configuring notifications of events in the application operation" on page 132). By default, no notification recipients are specified.

You can edit the text in the automatic notification of events that are logged by anti-virus scanning and content filtering. When making templates for notifications about events related to on-access and on-demand scans, you can use the following variables:

Table 7. Variables in notification templates

Variable name	Variable value
%ACTION%	The application's action on the object.
%AUTHOR%	Name of the user who is the file author. If the user cannot be recognized (e.g., during an on-demand scan), the variable takes on the value `n/a`.
%BACKUP_RESULT%	Object backup result.
%FARM_NAME%	Name of the server farm associated with the event.
%FILE_NAME%	Name of the object scanned by the application.
%FILE_URL%	Path to the object on SharePoint.
%FILE_VERSION%	Version of the file scanned by the application. This variable can only be used in notifications about events of an on-demand scan.
%INCIDENT_ID%	Unique ID of the incident. The ID allows finding information about the event in the application event log and Backup.
%LAST_MODIFIER%	Name of the user who has been the last to make any changes to the file. If the user cannot be recognized (e.g., during an on-demand scan), the variable takes on the value `n/a`.
%ODS_TASK_NAME%	Name of an on-demand scan task. This variable can only be used in notifications about events of an on-demand scan.

Variable name	Variable value
%OPERATION_TYPE%	The user's action on the object (e.g., downloading the file from a SharePoint website to the user's computer). This variable can only be used in notifications about events of an on-access scan.
%SERVER_LOCAL_DATETIME%	Date and time the malicious object or unwanted content was detected on the server. The variable takes on the value of the local time of the server.
%SERVER_NAME%	Name of the server associated with the event.
%THREAT_DESCRITION%	Name of the virus or category of unwanted words and phrases.
%USER%	Name of the user associated with the event. This variable can only be used in notifications about events of an on-access scan.
%UTC_OFFSET%	Time shift regarding UTC (Coordinated Universal Time).

For other events (such as changes in the database status and condition, or license-related events), the notification text remains unchanged.

Notifications about license-related events

Kaspersky Security checks licenses of Security Server and the DLP Module after each database update. The application sends notifications about license-related events in the following cases:

- If the license expires soon

  The application sends the notification once per day (at 12:00 A.M. UTC) if both the active key and the additional key expire. By default, the application starts sending notifications 15 days before this event. You can change the term for sending the license expiration notification (see section "Changing the term of sending license expiration notifications" on page 133).

- If the license already expired

The application sends the notification once per day (at 12:00 A.M. UTC) if the active key expired and no additional key is available.

- If the active key has been added to the black list of keys

  When updating anti-virus databases, the application checks the black list of keys for active keys. The application sends a notification if at least one active key has been found in the black list of keys.

Kaspersky Security sends special notifications about events related to Security Server and DLP Module licenses.

SMTP server configuration for delivery of notifications

► *To define the SMTP server settings for sending notifications:*

1. In the Administration Console tree, select the protected SharePoint server on which you want to configure the SMTP server.
2. In the node tree of this server, select the **Notifications** node.

   The workspace of this node displays the notification settings.
3. Configure the following settings in the **SMTP server settings** section:
   - Email addresses of SharePoint administrators.

     The application sends any notifications of application operation events to those addresses. You can configure notifications in the **Notifications** node.

     Use a semicolon to separate email addresses in the entry field.

     No addresses are specified by default.
   - Email address from which the application will send notifications of events in the application operation.

     By default, the application sends email messages from the email address, which is specified in the SMTP server settings on SharePoint.

4. Select the method of SMTP server configuration from the following options:

    - **Use SMTP server settings on SharePoint**.

      The application uses the settings of the SMTP server defined on SharePoint. If the settings of the SMTP server have not been defined on SharePoint, the application will not be able to send email messages.

      This is the default option.

    - **Use custom SMTP server settings**.

      The application uses the settings of the SMTP server that have been specified manually.

      If you select this option, the **SMTP server address**, **Account**, and **Password** fields become available. In this fields, you can specify the settings of the SMTP server that you intend to use for sending email messages.

5. If you need to test the operation of the SMTP server that has been configured manually, click the **Send test message** button.

6. Click the **Save** button in the upper part of the window.

The application saves the SMTP server settings for sending notifications.

Configuring notifications of events in the application operation

► *To configure automatic notifications of events in the application operation:*

1. In the list of protected servers that have been added to Administration Console, select the SharePoint server on which you need to configure notifications of events in the application operation.

2. In the node tree of this server, select the **Notifications** node.

   The workspace of this node displays the notification settings.

3. In the **Event notifications** section, configure notifications as follows:

    a. In the left part of the section, in the **Notification subjects** list, select an event of which the application will notify you by email.

    The right part of the section displays a list of recipients that can be sent notifications.

    b. Select the check box next to the recipients that will be automatically notified of this event by the application. You can specify the following recipients:

    - **Administrator**. Email address(es) of the administrators specified in the **Event notifications** section.
    - **Author**. Email address of the document author (user who uploaded the first version of this document to SharePoint). The author's email address is contained in the settings of the SharePoint server on which the document is stored.
    - **User**. Email address of a user associated with the event. The user's email address is contained in the settings of the SharePoint server on which the document is stored.
    - **Additional addresses**. Email address(es) specified in the entry field. Use a semicolon to separate email addresses in the entry field.

    c. If necessary, edit the notification text by clicking the **Template** button.

4. Click the **Save** button in the upper part of the window.

The settings of notifications about events in the application operation will be saved.

Changing the term of sending license expiration notifications

► *To change the term of sending license expiration notifications:*

1. In the list of protected servers that have been added to Management Console, select the SharePoint server on which you need to configure license expiration notifications.

2. In the node tree of this server, select the **Notifications** node.

    The workspace of this node displays the notification settings.

3. In the left part of the **Event notifications** section, in the **Notification subjects** list, select **License-related events**.

   The right part of the section then displays the settings of license-related event notifications.

4. In the **Notify about license expiry in** spin box, specify how many days before the license expiration the application must start sending notifications.

   By default, the application sends the first notification 15 days before the license expires.

   > Notifications are sent once per day (at 12:00 A.M. UTC).

5. Click the **Save** button in the upper part of the window.

The notification settings are saved. The application starts sending license expiration notifications on the specified day.

Backup

This section contains information about Backup, provides instructions on managing copies of files moved to Backup and configuring Backup settings.

In this section

About backup

Kaspersky Security saves in Backup copies of files that require action based on the results of Anti-Virus scanning and / or Content filtering (such as blocking or deletion). The application places in Backup copies of all harmful files, whether they can be disinfected or not.

Kaspersky Security places files to the Backup storage in encrypted form, which prevents the infection risk (files in Backup storage are not accessible without decryption).

Backup size

The data volume that can be stored in the Backup may be restricted by one of the two following parameters:

- Total number of files in Backup cannot exceed 50000. You cannot remove or change this restriction.
- The default size of Backup is 3686 MB. You can change the size of backup (see section "Configuring automatic backup clearing" on page 120).

Removing files from Backup

The application periodically (every time a new file is placed in Backup) checks compliance with the set restrictions on the size of Backup.

If the restrictions are exceeded, the application:

- Stops placing files in Backup, if the number of files in storage is exceeded.
- Frees up the necessary disk space by deleting the oldest files, if the restriction on storage size is exceeded by the addition of another file. The files stored for the longest amount of time are deleted first.

You can also delete files from Backup manually. For example, you may need to delete files that have been successfully restored after disinfection, or delete all files to purge Backup.

Operations with objects placed in Backup

You can perform the following actions on objects stored in Backup:

- View a list of files with detailed information about files placed in Backup in table form;
- Use the quick search function or extended filter to find the files in the list;
- Restore files, for example, if you want the application to rescan them using an updated version of the databases;
- Save files to the local drive on your computer, for example, to inspect them more closely;
- Delete files from Backup that are no longer needed;
- Purge Backup by deleting all files from it.

In this section

Viewing the list of files in Backup

You can view the list of files in Backup; it is displayed as a table with corresponding column headers.

► *To view the list of files in Backup:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Backup** node.

   The workspace displays information about Backup and a list of files moved to Backup.

   The top right corner of the workspace displays the number of files moved to Backup and the total size of these files.

   The bottom right corner of the workspace displays the following information:

   - The range of lines in the table listing files.
   - The number of lines in the table listing files.
   - The page number of the files list.

   In the files list you can view the information about files stored in Backup. The appearance of the files list may differ depending on the columns selected for display.

   By default, the list contains the following file information:

   - **File name**. File name.
   - **Path to file**. The path to the original location of the file on the server.
   - **Account**. Account of the user who had performed the operation that resulted in file addition to Backup.

- **Restored**. Date and time of file restoration on server.
- **Detected**. Date and time of object detection in file.
- **Component**. The module, that scanned the file - anti-virus scan or content filtering.
- **Reason why moved to Backup**. Name of the object detected in the file.
- **Scan type**. The type of scan which detected the object – on-demand or on-access scan.

2. Configure the appearance of the files list (if necessary) by selecting the columns to be displayed in the table:

   a. Click the **Select columns** button.

   This opens the **Select columns to display** window.

   The columns in the table of files will appear and disappear as you select or clear their corresponding check boxes.

   > The **File name** column is always displayed. It cannot be hidden.

   b. Click outside the **Select columns** window to close it.

3. You can sort the files list in the table by any of the columns in ascending or descending order, as required. To do this, click the header of the column that you want to sort files by, for example, **File name**, **Path to file**, or **Component**. If you want to reverse the sorting order, click the header once again.

   The list of files will be sorted by the selected column. The sorting symbol will appear in the header of the selected column:

- ▼ – sorted in ascending order
- ▲ – sorted in descending order

To view the details of a specific file, select it in the file list using the buttons to navigate to the next / previous, first / last pages of the file list « ‹ 1 › ». To find files in the list, you can also use the quick search (see section "Quick file search in backup" on page 139) and extended filter functions (see section "Extended file search in backup" on page 140).

Quick file search in Backup

► *To quick-search files in Backup:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Backup** node.

   The workspace displays a list of files moved to Backup.

2. Enter the pattern string for file search in the **Quick search** field. The pattern string supports masks.

   Quick search begins acting immediately as soon as you enter the template string.

   The table lists only files that match the search condition. A file will match the search condition if the entered pattern string can be found in at least one of the following file properties:

   - **File name**
   - **Path to file**
   - **Account**
   - **Owner**
   - **Owner email**
   - **Last edit by**
   - **Last editor email**
   - **ID**.

If you want to cancel quick search, click the ☒ icon next to the **Quick search** field.

Extended file search in Backup

► *To find files in Backup using the extended filter:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Backup** node.

   The results window will display the list of files stored in Backup.

2. Click the ⌄, icon to maximize the extended filter section.

   The extended filter section will be displayed. The section contains the list of filter conditions. By default, the list contains three lines where you can specify the conditions that will be used to filter document copies. Each filter condition consists of three parts: the file property to check, the pattern string and the comparison rule applied while matching the property and the pattern string.

3. To define a filtration condition:

   a. Select the property to check from the drop-down list in the left part of the line.

   You can pick any of the following values as the property to check:

   - **File name**
   - **Path to file**
   - **User name**
   - **Account**
   - **ID**
   - **Owner**
   - **Owner email**
   - **Last edit by**
   - **Last editor email**
   - **Scan type**.

   b. Select the comparison rule from the drop-down list in the middle of the line.

   The set of values in the list will correspond to the selected value of the property to check. For example, when checking the **File name** property, the list contains the following values: **Includes**, **Does not include**, **Empty field**.

> If you have selected **Empty field**, the entry field in the right part of the line will become inactive.

c. Enter the template string in the entry field in the right part of the line. The pattern string supports masks.

Specified filter condition will be applied to the list of files in Backup immediately as soon as you specify all its three parts. The files list only displays files matching all specified filtering conditions.

4. If you need to define more than three filter conditions, you can append additional lines to the list of conditions. To do this, click the **Add a condition** button.

   A new line will appear in the lower part of the filter conditions section.

5. If you want to delete an additional filter condition, click the ✖ icon in the filtering condition line.

   The selected line will be deleted from the list of filter conditions. The list of files will be refreshed to match the remaining filter conditions.

For convenience, you can minimize the extended filter section by clicking the ▲ icon. Minimized extended filter will continue to function. If you want to cancel extended filtering, click the **Reset filter** link.

Restoring files from backup

► *To restore files from Backup:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Backup** node.

   The workspace displays a list of files moved to Backup.

2. Select the files that you want to restore in the table.

   > Restoring files containing viruses and malicious objects can cause the computer to be infected.

3. Click the **Restore** button.

   Selected files will be decrypted and restored to the original locations in SharePoint structure. The files will be restored in the same format and under the same names they had when they were added to Backup.

   While restoring objects, the application updates in SharePoint the following relevant information:

   - **Account**. The application records to the field the account name of its administrator.
   - **Comments**. The application records in this field the application name, date when an object was placed in Backup and file version.
   - **Version**. The application updates the file version.

   After file restoration its copy and relevant information remains in Backup.

Rules for restoring files when version control is enabled in SharePoint

When files are being restored from Backup, it is possible that the path specified in SharePoint points to a file of the same name. Restoration of files of the same name depends on version control settings configured on the SharePoint server.

The following version control options exist:

- *Major*. File versions are available to all users of the SharePoint server.
- *Minor*. File versions are available to a limited group of users.

Restoring a file of the same name with version control enabled

If there is no file of the same name in SharePoint, the application restores the object from Backup as a file with the first minor or major version, depending on the version of the file when a copy of it was placed in Backup. If major version control is enabled in SharePoint, the file will be restored as a file with the corresponding major version.

If there is a file of the same name in SharePoint, Kaspersky Security restores the file according to the following rules:

- Kaspersky Security restores the new minor version if minor/major version control is enabled in SharePoint and the file in Backup has a minor version.
- Kaspersky Security restores the new major version in all other cases.

> If the file being restored has no version, the application restores the file as a file with a new minor version (if minor/major version control is enabled in SharePoint), or as a file with a new major version (if major version control is enabled).

Restoring a file of the same name with version control disabled

In this instance, Kaspersky Security prompts you to replace the file of the same name with the file being restored.

You can select one of the following actions in the window with the prompt to replace the file:

- **Yes**. The file in SharePoint is replaced with the file being restored.
- **No**. The file in SharePoint is not replaced with the file being restored. In this case, the file being restored remains in Backup.

When several files are being restored from Backup and there is a file of the same name of at least one of them in SharePoint, Kaspersky Security prompts you to replace the file / files of the same name with the file / files being restored.

You can select one of the following actions in the window with the prompt to replace the file / files:

- **Yes, restore the file**. The file in SharePoint will be replaced with the restored file.
- **No, do not restore the file**. The file in SharePoint will not be replaced with the restored file.

Saving files from Backup to disk

► *To save files in Backup to disk:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Backup** node.

   The results window will display the list of files stored in Backup.

2. If you want to save a single file to disk:

   a. Select in the files list the file, which you want to save to disk. You may use quick search or extended filter to find the file.

   b. Click the **Save** button.

   The standard file saving dialog will appear.

   c. Select the destination folder for the file.

   d. If you want to save the file under a different name, enter one in the **File name** field.

   e. Click the **Save** button.

   Selected file will be saved in the destination folder.

3. If you want to several files to disk:

   a. Select in the list the files, which you want to save to disk. You may use quick search or extended filter to find the files.

   b. Click the **Save** button.

   The standard destination selection dialog will appear.

   c. Select the destination folder where you want to save the files and click **Save**.

   Selected files will be saved in the destination folder.

Removing files from backup

► *To delete files from Backup:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Backup** node.

   The results window will display the list of files stored in Backup.

2. Select in the list the files, which you want to delete. You may use quick search or extended filter to find the files.

   > Kaspersky Security permanently removes files from Backup.

3. Click the **Delete** button.

   A warning dialog will appear.

4. Click the **Yes** button.

   Selected files will be deleted from Backup.

Purging Backup manually

You can purge Backup by deleting all the objects inside it.

► *To purge the Backup:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Backup** node.

2. In the workspace, click the **Purge Backup** button below the list of files moved to Backup.

   The application permanently deletes all files in Backup.

Managing reports

This section describes operational reports, and contains guidelines on how to configure report content and report schedules.

In this section

About reports

Kaspersky Security allows you to generate anti-virus protection, content filtering and operational reports. Reports allow you to analyze information about the protection status of a SharePoint server. Reports provide information on the number of clean and infected files and the number of files disinfected and removed.

Ready reports are displayed in the workspace of the **Reports** node, on the **View and generate reports**tab. You can view the report in the web browser window (see section "Viewing ready reports" on page 150).

You can generate reports using one of the two following methods:

- Generate reports manually

  The application generates a report upon your request (see section "Generating reports manually" on page 147)

- Generate reports through a report task

  The application generates reports automatically according to the specified task settings (see section "Creating a report generation task" on page 148). You can set up a report generation schedule or delivery of notifications about created reports by email (see section "Configuring a report generation task" on page 149). If necessary, you can run report generation tasks manually (see section "Starting a report generation task" on page 148).

  The list of report generation tasks is displayed in the workspace of the **Reports** node on the **Report creation tasks** tab. Report generation tasks that were or could not be run at the scheduled time are highlighted red.

If a report generation task has not been executed, information about this event is displayed in the list of tasks, in the **Status** column:

- **Deleted: <Server name>**. Security Server of Kaspersky Security has been deleted from the SharePoint server specified in the report generation task settings. You can specify a different SharePoint server in the task settings.

- **Task not executed**. The SharePoint server specified in the report generation task settings was not available at the time scheduled for the start of the task. The availability of the server needs to be checked.

Generating reports manually

► *To generate a report manually:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Reports** node.

2. In the workspace, on the **Reports** tab, click the **New report** button.

   This opens the **Report settings** window.

3. Select one of the following reporting periods:

   - **For 24 hours**. The application creates a report for the selected day.
   - **For period**. The application creates a report for the selected time period.

4. Click the **OK** button.

The report will be displayed in the list of generated reports in the **View and generate reports** section.

Creating a report generation task

► *To create a new report generation task:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Reports** node.
2. In the workspace of the **Reports** node, on the **Report creation tasks** tab, click the **Create** button.

   The **Task settings** window opens, which allows you to define the settings for the report creation task.

3. In the **Task settings** window, define the settings for the report creation task, then click **OK**.

   The task that you have created will be added to the list of tasks in the workspace. If necessary, you can edit the task settings (see the section "Configuring a report generation task" on page 149).

Starting a report generation task

► *To start a report generation task:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Reports** node.
2. In the workspace of the **Reports** node, on the **Report creation tasks** tab, select the relevant report creation task from the list.
3. Click the **Run task on server** button.

Configuring a report generation task

► *To configure a report generation task:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Reports** node.

2. In the workspace of the **Reports** node on the **Report creation tasks** tab, select the task whose settings you want to modify, and click the **Change** button.

   This opens the **Task settings** window.

3. In the **Task settings** window, define the following settings:

   - In the **Task name** field, edit the task name.

   - Select the **Run on schedule** check box if you want the application to generate the report upon a schedule, and select from the dropdown list the server on which the task will run. In the **Schedule** section, set up a schedule for the task run:

     - **Every N days**. The report will be created at the interval with the specified number of days, at the specified time. The report contains data for the last N days (by default, collected from 12:00 AM of the first day of the interval to 12:00 AM of the report generation day). You can change the report generation time in the **Start time** entry field.

     - **Weekly**. The report will be created at the defined time on the specified day of the week. The report contains data for the last 7 days (by default, from 12:00 AM of the first specified day of the week to 12:00 AM of the report generation day, for example, from Monday to Monday). You can change the report generation time in the **Start time** entry field.

     - **Monthly**. The report will be created at the defined time on the specified day of the month. The report contains data for the last month (by default, collected from 12:00 AM of the specified date of the previous month to 12:00 AM of the specified date of the report generation month). You can change the report generation time in the **Start time** entry field.

> The report generation schedule uses the time of the SharePoint server where the task is started.

- If you want reports to be sent to the administrator's email address, select the **Send to administrator** check box.
- If you want reports to be sent to other email addresses, select the **Send to recipients** check box and specify email addresses in the entry field. If several addresses are defined, use a semicolon as a delimiter.

4. To save the changes and close the window, click **OK**.

Deleting a report generation task

► *To delete a report generation task:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Reports** node.
2. In the workspace of the **Reports** node on the **Report creation tasks** tab, select in the list the task that you want to delete, and click the **Delete** button.

Viewing ready reports

► *To view a ready report:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Reports** node.
2. On the **Reports** tab, select in the list the report that you want to view and click the **View** button.

   The report opens in the default browser.

   The report contains the following information:

   - Date and time of report generation.
   - Name of the SharePoint server for which the report has been generated.

- Reporting period covered by the report.

Report on operations with files. Information on the number of files processed by Kaspersky Security:

- **Files submitted for scanning during the reporting period**. Files submitted for scanning during the reporting period.
- **Recognized as clean**. Number of files recognized as clean after being scanned by application components to which they were referred for scanning.
- **Disinfected**. Number of files that have been successfully disinfected by the application.
- **Deleted**. Number of files that have been deleted after scanning.
- **Blocked**. Number of files that have been blocked during on-access scanning.
- **Skipped (threat detection only)**. Number of files that have been skipped by the application after anti-virus scanning and content filtering according to the configured settings of on-demand and on-access scanning.
- **Not processed**. Number of files that have not been scanned by at least one Kaspersky Security component.

Report on status of server protection:

- **Files received for Anti-Virus scanning during the reporting period**.
- Status labels assigned by the application to files as a result of virus scanning:
  - **Non-infected**. Number of files that have been found to be free from threats during virus scanning.
  - **Infected**. The number of files with a code segment fully matching a code segment of a known application posing a threat.
  - **Probably infected**. The number of files whose code contains a modified segment of code of a known application posing a threat, or files resembling such application in the way it they behave.
  - **Password protected**. Number of password-protected archives.
  - **Corrupted**. Number of files that cannot be read by Kaspersky Security.

Information about skipped files:

- **Excluded from scanning by the Administrator**. Number of files that have been skipped according to the virus scan exclusion settings.
- **License issues**. The number of files that have not be scanned due to license errors (such as a missing key).
- **Processing error**. Number of files that have been skipped due to errors during virus scanning.

Operations on malicious files:

- **Disinfected**. Number of files disinfected after virus scanning.
- **Deleted**. Number of files deleted after virus scanning.
- **Blocked**. Number of files blocked after virus scanning.
- **Skipped (threat detection only)**. The number of files that, although found to contain a threat during an anti-virus scan, have been skipped because the **Skip** action had been specified in the scan settings.

Content filtering report:

- **Files received for Content filtering during the specified time period**.
- Status labels assigned by the application to files as a result of content filtering:
  - **Allowed**. Number of files that have been found to be free from violations of content filtering policies.
  - **Forbidden format**. Number of times that the content filtering component detected prohibited file formats specified in the content filtering settings.
  - **Forbidden mask**. Number of times that the content filtering component detected file names that match masks specified in the content filtering settings.
  - **Forbidden content**. Number of times that the Content filtering component detected words or phrases included in Kaspersky Lab sections and user categories within the search scope configured in the Content filtering settings

> If one and the same file causes multiple detections by the content filtering component in a number of categories, each detection is recorded under the corresponding category.

Information about skipped files:

- **Excluded from scanning by the Administrator**. Number of files that have been skipped according to the content filtering exclusion settings.
- **Text extraction errors**. Number of files whose contents have not been scanned by the application due to text extraction errors. Such errors may be caused by errors in the corresponding filter of IFilter Utility or a stopped Kaspersky Text Extracting Service.
- **License issues**. The number of files whose content has not been scanned by the applications to due license violations, such as a missing or blacklisted key.
- **Text filter is not available**. Number of files whose contents have not been scanned by the application because the corresponding filter of IFilter Utility is disabled or not installed.
- **Processing error**. Number of files that have been skipped due to other errors occurring during content filtering.

Actions taken by the application on files found to contain unwanted content.

- **Deleted**. Number of files for which the action is set to **Delete** in content filtering settings.
- **Blocked**. Number of files for which the action is set to **Block** in content filtering settings.
- **Skipped (threat detection only)**. Number of files for which the action is set to **Skip** in content filtering settings.

SharePoint web objects scan report:

- **SharePoint web objects submitted for Content filtering during the reporting period**.

- Actions taken by the application on SharePoint web parts based on the results of content filtering:
  - **Recognized as clean**. Number of SharePoint web parts that have been found to be free from violations of content filtering policies.
  - **Blocked**. Number of SharePoint web parts that have been blocked based on the results of content filtering.
  - **Skipped (threat detection only)**. The number of SharePoint web objects that, although found to contain unwanted content, have not been blocked because the **Skip** action has been specified for them in the scan settings.

  In on-demand scan mode, the application always skips web objects that contain unwanted content even if the **Block** action is configured in task settings.

- Information on skipped SharePoint web objects:
  - **License issues**. The number of SharePoint web objects that have not be scanned due to license errors (such as a missing key).
  - **Processing error**. The number of SharePoint web objects that have been skipped due to errors occurring during content filtering.

Application logs

This section provides information about the logs of Kaspersky Security and how to define the settings for maintaining those logs.

In this section

About logs

Details of the application operation are recorded into Kaspersky Security logs (hereinafter referred to as "logs") and into Microsoft Windows Event Log.

About Windows Event Log

Details of the application operation in Windows Event Log are recorded by Kaspersky Security services (see page 46). For events related to the activities of Kaspersky Security, the **Source** column indicates the name of the service that has detected those events. The names of all the services start from "KSH".

About event logs in Kaspersky Security

Details of the application operation in Kaspersky Security logs are recorded by the application's components and software modules. The application records information to the end of the most recent log. Records of new events are grouped at the top of the list. When the log reaches100 MB in size, the application archives it and creates a new one.

Event logs are created in TXT format and saved to the default folder <Application installation folder>/Logs.

You can define the following settings of Kaspersky Security logs:

- Time for storage of logs (see the section "Configuring the log storage term" on page 119)
- Level of detail for logs (see the section "Configuring the detail level of event logs" on page 119)
- Location of the folder that Kaspersky Security uses to save logs (see the section "Configuring the path to the logs folder" on page 118).

You can also enable the logging of event details for the Content Filtering log.

> Data saved in a log may contain confidential information. For security reasons (for example, to prevent unauthorized access or possible data leaks), you are advised to personally protect files of the application log.

About the log of content filtering

The log of Content Filtering allows you to check if Content Filtering is configured properly.

The log of Content Filtering is located in the folder <Application installation folder>\logs\content_filtering\content_filtering_incidents_log_YYYYDDMM.csv, where YYYYDDMM stands for the log creation date.

> The log of Content Filtering is created on a daily basis and contains the details of content filtering incidents for the relevant day. Logs for the previous days are stored in the folder <Application setup folder>\logs\content_filtering in archives with the corresponding names.

When a Content Filtering incident is triggered by the name or the content of a file, the following details are recorded in the log of Content Filtering:

- Incident ID
- Path to the file

- File name
- The word or phrase that caused the Content filtering incident
- The Kaspersky Lab section or user category to which the specific word belongs

The log of Content Filtering will additionally record a sequence of characters from the text that has been extracted from the file or the field of a SharePoint web object by the corresponding filter of Kaspersky IFilter Utility.

When a content filtering incident is caused by the content of a SharePoint web part, the following details are recorded in the log of content filtering incidents:

- Incident ID
- Path to the SharePoint web object
- Name of the field of the SharePoint web object in which unwanted content has been detected
- The word that caused the content filtering incident
- The Kaspersky Lab section or user category to which the specific word belongs

For a more detailed check of the operation of Content Filtering, you can enable the detailed logging of events to the log of Content Filtering. The log records a sequence of 10 words located in the text before the word that caused the Content filtering incident, the word itself, and 10 words located in the text after the word that caused the incident. If these 10 words contain more than 100 characters, the sequence is limited to 100 characters before and after the word that caused the Content filtering incident.

> Data in the Content filtering log is not encrypted. For security reasons (for example, to prevent unauthorized access or possible data leaks), you are advised to personally protect files of the application log.

Configuring the log storage term

► *To configure the storage term for log files:*

1. Select and open in the Administration Console tree the node corresponding to the necessary SharePoint server. Then select the **Settings** node.

2. In the **Diagnostics** section, in the **Log storage period** field, specify a value for the log storage term (in days).

   The application will store logs during the specified number of days since the last record is added to the log. If no new records have been added to a log over the specified time period, the application deletes the log.

3. Click the **Save** button in the upper part of the window.

Configuring the path to the logs folder

► *To configure the path to the logs folder:*

1. In the Administration Console tree, select and open the node that corresponds to the relevant SharePoint server, then select the **Settings** node.

2. In the **Diagnostics** section, in the **Logs folder** entry field, specify the path to the logs folder.

   > Avoid using variables and masks when specifying the path to the folder. Do not specify an FTP server or a network folder as a location where the application logs are stored.

   The application will save logs using the specified path. If you configure the path to the folder on a server within a farm, the configuration will cover the entire server farm.

3. If necessary, click the **Default** link to restore the default path to the logs folder.

4. Click the **Save** button in the upper part of the window.

If the application does not save logs using the specified path, check the rights of access to that folder.

Configuring the detail level of event logs

► *To configure the detail level of event logs:*

1. In the Administration Console tree, select and open the node that corresponds to the relevant SharePoint server, then select the **Settings** node.
2. Click the **Settings** button in the **Log details** section.

   This opens the **Diagnostics settings** window.
3. Select events that must be recorded in detail.
4. Click **OK** 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 record main events in the application 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 changes to **Maximum**. The application will record detailed information about all events to logs.

   > When maintaining a log with the advanced detail level, this log contains web addresses that have been scanned for phishing.
5. If you want to reset the current detail level of a log, click the **Reset** button.

   The application changes the detail level to **Minimum**. Logs will only contain basic events from the application operation, such as scan results, updates of databases, and keys added.
6. If necessary, select the **Record details of events to Content Filtering log** check box.

   The application will record to the Content Filtering log a text fragment that is related to a content filtering event.
7. Click the **Save** button in the upper part of the window.

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

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 13), 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, please read the 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 Kaspersky Lab Technical Support through the Kaspersky CompanyAccount portal.

Technical support by phone

You can phone Kaspersky Lab Technical Support representatives in most regions. You can find information about ways of obtaining technical support in your region and the contacts of Technical Support on Kaspersky Lab Technical Support website» (http://support.kaspersky.com/support/contacts).

Before contacting Technical Support, read the technical 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) is a portal for companies that use Kaspersky Lab applications. The Kaspersky CompanyAccount portal is designed to facilitate interaction between users and Kaspersky Lab specialists via online requests. You can use the Kaspersky CompanyAccount portal 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 portal 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 Info Collector

When you inform Technical Support of the problem, you may be asked to create an archive with data on the operation of the application using the InfoCollector utility, and to send it to Technical Support.

To get acquainted with the description of the Info Collector utility and download the utility, please go to the Kaspersky Security page in the Knowledge Base (http://support.kaspersky.com/ksh9), section "Troubleshooting".

Glossary

A

Activating the application

Switching the application into full-function mode. Application activation is performed by the user during or after the application installation. You should have a key file to activate the application.

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 tools and enables configuration and management of the server component. The management module is implemented as an extension of the Microsoft Management Console.

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

A dedicated storage area intended for saving backup copies of objects that are created prior to their disinfection or removal.

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.

D

Disinfection

A method of processing infected objects that results in full or partial recovery of data. Not all infected objects can be disinfected.

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 CompanyAccount

Portal for sending requests to Kaspersky Lab and tracking the progress made in processing them by Kaspersky Lab experts.

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 cloud services, which provides access to the current knowledge base of Kaspersky Lab describing the reputation of files, websites 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.

Key file

A file with the .key extension that makes it possible to use a Kaspersky Lab application on the terms of a trial or commercial license. You have to specify the path to the key file after the application has been installed. You may use the application only when you have a key file.

L

License certificate

A document that Kaspersky Lab transfers to the user together with the key file or activation code. It contains information about the license granted to the user.

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.

O

Object removal

The method of processing objects which ends in it being physically deleted from its original location (hard drive, folder, network resource). We recommend that this method be applied to dangerous objects which, for whatever reason, cannot be disinfected.

On-demand scan

Kaspersky Lab's program operation mode initiated by the user and designed to scan and check any resident files.

On-access scan

A mode of a Kaspersky Lab application whereby files are scanned automatically on being uploaded to the server or downloaded from the server.

P

Phishing

A kind of online fraud aimed at obtaining unauthorized access to confidential data of users.

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.

S

SharePoint server structure

A tree of nodes that makes it possible to manage the content of a SharePoint server. In nodes, you can select elements and specify the actions to take on them.

Skipping of an object

Processing method in which an object is allowed to pass to the user unchanged. If event logging is enabled for this event type, information about the object detected will be logged in the report.

U

Unwanted content

Information that is unsuitable for various groups of users. Unwanted content includes websites and messages that propagate violence, incite acts of terror, contain child pornography or profanity.

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

Virus

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.

AO Kaspersky Lab

Kaspersky Lab software is internationally renowned for its systems of computer protection against various threats, including viruses, malware, spam, network and hacker attacks.

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). In Russia, according to IDC, Kaspersky Lab is the first choice among vendors of computer protection systems for home users (IDC Endpoint Tracker 2014).

Kaspersky Lab was founded in Russia in 1997. Today, Kaspersky Lab is an international group of companies running 34 offices in 31 countries. The company employs more than 3000 qualified specialists.

PRODUCTS. Kaspersky Lab's products provide protection for all systems—from home computers to large corporate networks.

The personal product range includes applications that provide data security for desktop, laptop, and tablet computers, and for smartphones and other mobile devices.

The company offers solution and technologies for control and protection of workstations and mobile devices, virtual machines, file servers and web servers, mail gateways, and firewalls. The company's portfolio also includes dedicated products for protection against DDoS attacks, protection of environments managed with industrial control systems, and fraud prevention. Used in conjunction with Kaspersky Lab's centralized management system, these solutions ensure effective automated protection for companies and organizations of any scale 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 thousands of new computer threats, create tools to detect and disinfect them, and include them in the databases used by Kaspersky Lab applications.

TECHNOLOGIES. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. It is no coincidence that the program kernel of Kaspersky Anti-Virus is integrated into products by many other software vendors, such as Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, General Dynamics, Facebook, Juniper Networks, Lenovo, H3C, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, and ZyXEL. 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, according to tests and researches conducted in 2014 by the renowned Austrian anti-virus lab AV-Comparatives, Kaspersky Lab shared the leadership in the number of Advanced+ certificates awarded, which brought the Top Rated certificate to the company. But Kaspersky Lab's main achievement is the loyalty of its users worldwide. The company's products and technologies protect more than 400 million users, and its corporate clients number more than 270,000.

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.

Google Chrome is a trademark owned by Google, Inc.

Active Directory, Internet Explorer, Microsoft, SharePoint, SQL Server, Windows, Windows Server, Windows Vista and Windows PowerShell are trademarks of Microsoft Corporation registered in the USA and other countries.

Firefox, Mozilla are trademarks of the Mozilla Foundation.

Index