Kaspersky Security 8.0 for SharePoint Server

Installation Guide

APPLICATION VERSION: 8.0

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.

Document revision date: 10/3/2013

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

TABLE OF CONTENTS

ABOUT THIS GUIDE

This document is the Installation Guide for Kaspersky Security 8.0 for SharePoint Server® (hereinafter "Kaspersky Security" or "application").

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

A specialist installing the application must be skilled in administering the operating system, installing and configuring software. The specialist must review this Guide before installing the application.

This Guide is intended to do the following:

- Describe the preparation for Kaspersky Security installation, the application installation and activation process.
- Give advice on preparing the application for operation.
- Describe additional sources of information about the application and ways of receiving technical support.

IN THIS SECTION:

IN THIS DOCUMENT

Installation Guide for Kaspersky Security consists of the following sections:

Sources of information about the application (see page 8)

This section describes sources of information about the application and lists websites that you can use to discuss the application's operation.

Kaspersky Security 8.0 for SharePoint Server (see page 10)

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 support installation.

Preparing to install (see page 16)

This section describes how you can prepare the computer for installation of the application: create an account, grant this account privileges to install the application and manage Kaspersky Security, as well as create a database for storing configuration files.

Upgrading from an earlier version of the application (see page 19)

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

DOCUMENT CONVENTIONS

The document text is accompanied by semantic elements to which we recommend paying particular attention: warnings, hints, and examples.

Document conventions are used to highlight semantic elements. Document conventions and examples of their use are shown in the table below.

Table 1. Document conventions

SAMPLE TEXT	DOCUMENT CONVENTIONS DESCRIPTION
Note that...	Warnings are highlighted in red and boxed. Warnings provide information about possible unwanted actions that may lead to data loss, failures in equipment operation or operating system problems.

SAMPLE TEXT	DOCUMENT CONVENTIONS DESCRIPTION
It is recommended to use...	Notes are boxed. Notes may contain useful tips, advice, specific values of settings or important particular cases in the operation of the application.
Example: ...	Examples are given on a yellow background under the heading "Example".
Update means... The *Databases are out of date* event occurs.	The following semantic elements are italicized in the text: • New terms • Names of application statuses and events.
Press **ENTER**. Press **ALT**+**F4**.	Names of keyboard keys appear in bold and are capitalized. Names of keys that are connected by a + (plus) sign indicate the use of a key combination. Those keys must be pressed simultaneously.
Click the **Enable** button.	Names of application interface elements, such as entry fields, menu items, and buttons, are set off in bold.
➧ *To configure a task schedule:*	Introductory phrases of instructions are italicized and are accompanied by the arrow sign.
Enter help in the command line The following message then appears: Specify the date in dd:mm:yy format.	The following types of text content are set off with a special font: • Text in the command line • Text of messages that the application displays on screen • Data that the user must enter.
<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 describes sources of information about the application and lists websites that you can use to discuss the application's operation.

You can select the most suitable information source, depending on the issue's level of importance and urgency.

IN THIS SECTION:

SOURCES OF INFORMATION FOR INDEPENDENT RESEARCH

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

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

If you cannot find a solution for your issue, we recommend that you contact Kaspersky Lab Technical Support (see the section "Technical support by phone" on page 32).

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

Application page on the Kaspersky Lab website

The Kaspersky Lab website features an individual page for each application.

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

Application page on the Technical Support website (Knowledge Base)

Knowledge Base is a section of the Technical Support Service website that provides recommendations on how to work with Kaspersky Lab applications. Knowledge Base comprises reference articles that are grouped by topic.

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

Articles may provide answers to questions that are out of scope of Kaspersky Security, being related to other Kaspersky Lab applications. They also may contain news from the Technical Support Service.

Online help

The online help of the application comprises help files.

Online help contains information about each window of the application: the list of settings, their descriptions and links to the tasks using these settings.

Full help provides information about managing computer protection, configuring the application and solving typical user tasks.

Documentation

The package of application manuals includes the following documents: *Installation Guide for Kaspersky Security 8.0 for SharePoint Server* and *Administrator's Guide to Kaspersky Security 8.0 for SharePoint Server* (this Guide). These manuals will help you to install and activate the application on local area network computers, configure application settings, and find tips on using the application.

The latest versions of the manuals are available on the update download page (http://www.kaspersky.com/product-updates/sharepoint-security).

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.

CONTACTING THE SALES DEPARTMENT

If you have any questions on how to select, purchase, or renew the application, you can contact our Sales Department specialists in one of the following ways:

- By calling our HQ office in Moscow by phone (http://www.kaspersky.com/contacts).
- By emailing your question to sales@kaspersky.com.

The service is provided in Russian and English.

CONTACTING THE TECHNICAL WRITING AND LOCALIZATION UNIT

To contact the Technical Writing and Localization Unit, send an email to docfeedback@kaspersky.com. Please use "Kaspersky Help Feedback: Kaspersky Security 8.0 for SharePoint Server" as the subject line in your message.

KASPERSKY SECURITY 8.0 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 files and web objects hosted by SharePoint servers as they are uploaded to the server or downloaded from the server to the user's computer.
- Scan files and web objects hosted by SharePoint servers manually or schedule an automatic scan.
- Configure the scanning of SharePoint web objects: create custom scan categories, specify the type and format of unwanted files, and create masks of unwanted file names.
- Configure application actions on files containing malicious objects and web objects containing unwanted content or malicious and phishing URLs.
- Specify areas in the tree of SharePoint server nodes that need scanning, and exclude certain areas from the scan scope to ease the load on the server.
- Use Kaspersky Security Network to increase the effectiveness of protection of SharePoint servers.
- Scan files for malicious code that exploits system vulnerabilities.
- Save copies of the documents in Backup before disinfecting or deleting them.
- Generate reports on the results of scanning of files and SharePoint web objects manually or automatically according to schedule.

IN THIS SECTION:

DISTRIBUTION KIT

You can purchase the application through Kaspersky Lab's online stores (for example, http://www.kaspersky.com, in the **eStore** section) or partner companies.

Kaspersky Security 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).

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

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

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

SERVICE FOR USERS

By purchasing a license for the application, you can benefit from the following services during the entire term of the license:

- Database updates and new versions of the application
- Advice on issues related to the installation, configuration and use of the application by phone or via em ail
- Announcements of new Kaspersky Lab releases and information about new viruses and outbreaks To use this service, subscribe to news delivery from Kaspersky Lab on the Technical Support website.

Advice on issues related to operating systems and third-party applications and technologies is not provided.

HARDWARE AND SOFTWARE REQUIREMENTS

To ensure the application runs smoothly, the computer must meet the following minimum hardware and software requirements.

Hardware requirements

For SharePoint Server 2007:

- If installing Administration Console and Security Server:
  - Minimum 2.5 GHz processor (two 3 GHz processors or higher recommended)
  - 1 GB RAM (2 GB recommended)
  - 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 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:

- 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.

Software requirements

Required components to install the application:

- Microsoft SharePoint Server 2007, Microsoft SharePoint Server 2010 or Microsoft SharePoint 2013

  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 Server 2007
- Microsoft SharePoint 2010;
- Microsoft SharePoint 2013

Supported operating systems:

For SharePoint Server 2007 x86 / x64:

- If installing Administration Console and Security Server:
  - Windows Server® 2003
  - Windows Server 2003 x64
  - Windows Server 2003 R2

- Windows Server 2003 R2 x64
- Windows Server 2008
- Windows Server 2008 x64
- Windows Server 2008 R2
- Windows Server 2012 R2

- If installing only Administration Console:
  - Windows Server 2003
  - Windows Server 2003 x64
  - Windows Server 2003 R2
  - Windows Server 2003 R2 x64
  - Windows Server 2008
  - Windows Server 2008 x64
  - Windows Server 2008 R2
  - Windows Server 2012 x64
  - Windows Server 2012 R2
  - Microsoft Windows® XP x64 Service Pack 2
  - Microsoft Windows XP Service Pack 3
  - Microsoft Windows Vista® Service Pack 2
  - Microsoft Windows Vista x64 Service Pack 2
  - 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

For SharePoint Server 2010:

- If installing Administration Console and Security Server:
  - Windows Server 2008 x64

- Windows Server 2008 R2
- Windows Server 2012 R2

- If installing only Administration Console:
  - Windows Server 2003
  - Windows Server 2003 x64
  - Windows Server 2003 R2
  - Windows Server 2003 R2 x64
  - Windows Server 2008
  - Windows Server 2008 x64
  - Windows Server 2008 R2
  - Windows Server 2012 x64
  - Windows Server 2012 R2
  - Microsoft Windows XP x64 Service Pack 2
  - Microsoft Windows XP Service Pack 3
  - Microsoft Windows Vista Service Pack 2
  - Microsoft Windows Vista x64 Service Pack 2
  - 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

For SharePoint Server 2013:

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

- Windows Server 2003
- Windows Server 2003 x64
- Windows Server 2003 R2
- Windows Server 2003 R2 x64
- Windows Server 2008
- Windows Server 2008 x64
- Windows Server 2008 R2
- Windows Server 2012 x64
- Windows Server 2012 R2
- Microsoft Windows XP x64 Service Pack 2
- Microsoft Windows XP Service Pack 3
- Microsoft Windows Vista Service Pack 2
- Microsoft Windows Vista x64 Service Pack 2
- 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

Supported browsers:

- Windows Internet Explorer® 7.x (32-bit version)
- Windows Internet Explorer 7.x (64-bit version)
- Windows Internet Explorer 8.x (32-bit version)
- Windows Internet Explorer 8.x (64-bit version)
- Windows Internet Explorer 9.x (32-bit version)
- Windows Internet Explorer 9.x (64-bit version)
- Mozilla™ Firefox™ 3.6
- Google Chrome™ (last version)

PREPARING TO INSTALL

Before starting the installation, make sure that the following components are available on the computer on which Kaspersky Security is being installed:

- Microsoft .NET Framework 3.5 SP1. If the component is missing, the welcome window of the Kaspersky Security install package displays a link that can be followed to download and install the component.

  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. After rebooting the computer, you need to restart the installation of the application.

- Microsoft Management Console 3.0 (MMC 3.0). 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. To do so, follow the **Download and install MMC 3.0** link in the welcome window of the Kaspersky Security install package.

If Microsoft SharePoint Server 2007, 2010, or 2013, as well as Microsoft .NET Framework 3.5 SP1 and Microsoft Management Console 3.0 are installed on the computer, the installer prompts you to install Administration Console and Security Server.

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

Before installing Kaspersky Security on a standalone SharePoint server or a group of SharePoint farm servers, you must do the following:

- Create an account for Kaspersky Security.
- Assign the necessary rights to the account under which the installer is to be run.
- Create a database to store application and Backup configuration files.
- Assign the necessary rights to the account under which Kaspersky Security is to be administered.

Creating an account for using Kaspersky Security

Prior to installing Kaspersky Security, you have to create an account under which Kaspersky Security services will be run. This account must possess the following rights:

- Local Administrator on all servers where the application is to be installed
- SharePoint Farm Administrator
- Administrator rights for the SharePoint_Config and SharePoint_AdminContent_UID databases

  You can assign the account administrator rights for the specified databases in one of the following ways:

  - Assign the account the db_owner role using Microsoft SQL Server® Management Studio (or the utility Microsoft SQL Server Management Studio Express).
  - For each web application on the protected SharePoint portal, execute the following Microsoft PowerShell™ commandlet:

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

where WebApp is the name of the web application on the SharePoint server, and domain\KSH_User is the name of the account created for using Kaspersky Security.

Assigning rights to the account under which the installer is to be run

Assign the following rights to the account under which the application is to run:

- Local Administrator on the computer where the application is to be installed
- SharePoint Farm Administrator These rights are required to run the Application Configuration Wizard. Without these rights, the application installs successfully, but the Application Configuration Wizard is not available to configure the initial settings.
- Administrator rights for the SharePoint_Config and SharePoint_AdminContent_UID databases (as for the account created to run Kaspersky Security). Without these rights, configuring anti-virus settings of the SharePoint server is unavailable. At the final stage of the installation, when the files are being copied and the components registered, a 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.

Creating a database to store application and Backup configuration files

The database to be used by the application to store configuration and Backup data is created automatically during installation. To automatically create the database requires an account possessing the sysadmin role on the SQL server on which the database is to be created.

This account is used only to create the database during working the Setup Wizard. It is not used when installation of Kaspersky Security is complete.

The application can use a manually created database. In this case, the database must be created using the following script:

```
CREATE DATABASE [%database name%]

ON PRIMARY

(

NAME = [%database name%_

logical name of the primary data file ],

FILENAME = 'full path to the primary data file'

),

FILEGROUP [%database name%_BACKUP_DATA_FILE_GROUP]

(

NAME = [%database name%_BACKUP_DATA_FILE_GROUP],

FILENAME = 'full path to the secondary data file'

)
```

The account created to run Kaspersky Security must be assigned the db_owner role for the manually created database. At the Configuring SQL server connection stage of application installation (see section "Step 5. Configuring the connection between Kaspersky Security and SQL database" on page 24), specify this account in order to connect to the SQL server.

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

Kaspersky Security supports failsafe technologies for SQL databases. Detailed information about such support is available in the *Kaspersky Security Administrator's Guide*.

Assigning rights to the account under which Kaspersky Security is to be administered

To manage Kaspersky Security, the account under which Administration Console for Kaspersky Security is running must possess SharePoint Farm Administrator rights and read/write privileges for the Configuration folder in the application's installation folder (such rights are assigned by default to accounts with local administrator rights). Without these rights, services under Administration Console for Kaspersky Security are unavailable.

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

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 update 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 upgrades are available starting with application version 8.1.8481. Upgrades of earlier application versions are not supported.

The following update configurations of Kaspersky Security are available:

- Security Server and Administration Console installed on a standalone SharePoint server

  Before upgrading the 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.

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

During the update of the 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 accept the KSN agreement and I want to use KSN** check box is automatically cleared in Kaspersky Security settings. The procedure for enabling the KSN service is described in the *Administrator's Guide to Kaspersky Security 8.0 for SharePoint Server*.

During the update, the application databases are replaced with the ones from the update package. It is recommended that you update the databases immediately after the application update. The database update procedure is described in the *Administrator's Guide to Kaspersky Security 8.0 for SharePoint Server*.

STARTING THE APPLICATION UPGRADE

➧ *To start the procedure to update Kaspersky Security in any of the above configurations:*

1. If Kaspersky Security Administration Console is running on the computer for which you want to update the application, close this Administration Console before starting the update.

2. Run the file setup.exe in the distribution package of the application on the computer for which you want to update Kaspersky Security.

   This opens the welcome window of the install package.

3. Click the **Kaspersky Security 8.0 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 update of the application now starts.

5. When the update completes, the final screen of the Setup Wizard opens. To complete the update and close the Setup Wizard, click the **Finish** button.

Only Kaspersky Security version 8.1.8481 or later can be updated.

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

TIPS FOR UPDATING KASPERSKY SECURITY ON THE SHAREPOINT

When updating Kaspersky Security on the SharePoint farm, it is recommended that you complete the update in the shortest possible time frame.

If the update is performed in stages and continues for an extended period of time, the connection to Kaspersky Security Security Servers that have not been updated in order to change settings, view reports, create / change / run on-demand tasks or enable / disable on-access scanning needs to be made through the Administration Console that has also yet to be updated. The updated Security Servers used by Kaspersky Security should be managed via the updated Administration Console.

The updated version of Administration Console cannot connect to Kaspersky Security Security servers that have not been updated.

UPDATING KASPERSKY SECURITY ON A STANDALONE SHAREPOINT SERVER OR THE FIRST SERVER IN A SHAREPOINT FARM

After Security Server for Kaspersky Security and Administration Console have been upgraded on the first SharePoint server in a SharePoint farm or on a standalone SharePoint server, the following conditions apply:

- Files located in Backup before the application upgrade can be viewed, and all actions allowed by the application can be performed on them from the upgraded Administration Console connected to the upgraded Security Server.
- All reports created by the application before the update can be viewed from the updated Administration Console connected to the updated Security Server.
- All data on the operation of the application before the update is saved in the application's log file.
- The updated version of Kaspersky Security uses the active and additional keys added before the Security Server update. The validity period of the keys remains unchanged.

- The updated Security Server by default uses the same settings as the previous version.
- Operation statistics of Security Server for Kaspersky Security gathered before the application upgrade are not saved. As a result, reports generated after the upgrade of Kaspersky Security do not contain statistics of application operation before the upgrade, and the details pane of the **Control Center (<Server name>)** node in the **Statistics** section does not show data gathered before the application upgrade.

If the settings of the upgraded version of Kaspersky Security on the first server in the SharePoint farm are changed after the upgrade, for the remaining servers in the SharePoint farm (on which Kaspersky Security has not been upgraded) the application continues to use the settings that were configured during application setup on these SharePoint servers.

INSTALLING THE APPLICATION

This section includes step-by-step instructions for installing the application on the computer and information about system changes after installation of the application.

IN THIS SECTION:

SPECIAL CONSIDERATIONS OF INSTALLING THE APPLICATION

Kaspersky Security consists of two main components: the Security Server and Administration Console. The Security Server is always installed together with Administration Console on the same computer. Administration Console can be installed separately from Security Server on another computer to manage Security Server remotely.

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.

The Kaspersky Security installer is designed as a Wizard which provides information about the operations you must perform during each step of the installation procedure. This section describes the steps in the Setup Wizard.

STEP 1. INSTALLING THE REQUIRED COMPONENTS

➧ *To start the installation of Kaspersky Security,*

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

This opens the welcome window of the install package. In this window, you can perform one of the following actions:

- download and install the .Net Framework 3.5 SP1 component by following the link **Download and install .Net Framework 3.5 SP1** (if the component is not installed).

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

- start the Setup Wizard by following the link **Kaspersky Security 8.0 for SharePoint Server**.

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 License Agreement is concluded between the application user and Kaspersky Lab. By selecting the **I accept the terms and conditions of the License Agreement** check box, you confirm that you have read the License Agreement and accept its terms and conditions. You can print the text of the License Agreement by clicking the **Print** button.

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

STEP 3. SELECTING THE TYPE OF INSTALLATION

At this step, the Setup Wizard prompts you to select the type of installation that you require.

In the Setup Wizard window, you can select the type of installation:

- **Typical**. This installation uses the default paths to the installation and data storage folders. 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 24).

- **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 23).

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

STEP 4. SELECTING THE APPLICATION COMPONENTS

At this step, you can select the application components to be installed (Security Server and Administration Console or just Administration Console), and specify the paths to the installation and data storage folders.

To select the application components to be installed, and the paths to the installation and data storage folders:

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

   You can install Security Server and Administration Console, or just Administration Console. Only Administration Console is installed to manage Kaspersky Security Security Server 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 runtime and database logs for the application.

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

At this step in the Setup Wizard, you can configure a connection to link Kaspersky Security to the SQL database used to store configuration settings for the application and Backup data.

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.

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.

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 16).
   - The database created automatically by the Setup Wizard installer.
   - The database used by the previous version of the application (version 8.1.8481) – 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 16) 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 supports failsafe technologies for SQL databases. For details, see the *Administrator's Guide to Kaspersky Security 8.0 for SharePoint Server*.

STEP 6. SELECT AN ACCOUNT FOR RUNNING THE APPLICATION SERVICES KASPERSKY SECURITY

At this step, you need to specify the account to be used to run application services and connect Kaspersky Security to the SharePoint and SQL servers.

To select an account,

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 16).

STEP 7. COMPLETING INSTALLATION

At this step, the application files are copied to the computer, the components are registered in the system, and the installation is completed.

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 28). 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 SharePoint farm servers is enabled as soon as Kaspersky Security has been installed, but only if SharePoint farm server protection was enabled at the **Enabling protection** step of the Configuration Wizard (see section "**Step 2. Enable Anti-Virus protection**" on page 29) during application installation on the first farm server.

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.

Kaspersky Security folders

Table 2. Kaspersky Security folders created on the computer

FOLDER	KASPERSKY SECURITY FILES
%Kaspersky Security folder%; by default: • In Microsoft Windows 32-bit version – Program Files%\Kaspersky Lab\Kaspersky Security 8.0 for SharePoint Server\ • In Microsoft Windows 64-bit version – %Program Files(x86)%\Kaspersky Lab\Kaspersky Security 8.0 for SharePoint Server\	Kaspersky Security executable files, configuration, and logs (destination folder specified during installation)
• In Microsoft Windows 32-bit version – %Program Files%\Kaspersky Lab\Kaspersky Security 8.0 for SharePoint Server\data\ • In Microsoft Windows 64-bit version – %Program Files(x86)%\Kaspersky Lab\Kaspersky Security 8.0 for SharePoint Server\data\	Kaspersky Security updatable data
C:\Program Data\Microsoft\Windows\Start Menu\Programs\Kaspersky Security 8.0 for Microsoft SharePoint Server\	Kaspersky Security Administration Console, Administrator's Guide, and uninstaller shortcuts
C:\Windows\assembly\GAC_MSIL\SharePoint.Integration.Vsapi.Com	File to integrate Kaspersky Security with SharePoint

Kaspersky Security services

Table 3. Kaspersky Security services

SERVICE	PURPOSE
KSHSecurityService	The main Kaspersky Security service; manages Kaspersky Security tasks and processes
KSHIntegrationService	Service to integrate Kaspersky Security with SharePoint
KSHTextExtractorService	Service to integrate Kaspersky Security with IFilters
KSHAdministrationService	Service to manage Kaspersky Security and integrate it with the configuration

System registry keys

Table 4. 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
[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] [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\KSHTextExtractorService]	Kaspersky Security services

GETTING STARTED. APPLICATION CONFIGURATION WIZARD

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

IN THIS SECTION:

ABOUT THE APPLICATION CONFIGURATION WIZARD

The Application Configuration Wizard starts following installation of the application if Kaspersky Security is installed on a standalone SharePoint server or on the first server in a SharePoint farm server.

The Application Configuration Wizard helps to activate the application, enable anti-virus protection of SharePoint servers, and configure automatic database updates.

When the application is installed on subsequent farm servers, SharePoint users the settings configured using the Application Configuration Wizard on the first SharePoint farm server.

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.

Each step in the Application Configuration Wizard provides information about the actions that need to be taken.

STEP 1. ACTIVATING THE APPLICATION

To activate the application, you have to add a key. The key can be added after Configuration Wizard completion and application start. The key added during installation on the first SharePoint farm server is automatically used to install the application on subsequent SharePoint farm servers.

To add a key:

1. Click the **Add** button in the Application Configuration Wizard.
2. In the displayed **File name** dialog specify path to the key file (file with the .key extension) and click **Open**.

   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.

To delete a key,

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

STEP 2. ENABLE ANTI-VIRUS PROTECTION

The **Enable Anti-Virus protection and automatic database update** window lets you specify the anti-virus protection settings.

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

1. Select the **Enable protection** check box if you want Kaspersky Security to start performing on-access scanning at startup – anti-virus scanning and Content filtering of file content when you attempt to send a file from the computer to a SharePoint server or to download a file from the SharePoint server to the computer.

2. Select the **Enable automatic database updates** check box if you want the application to update the databases automatically as scheduled, or clear the check box if you want to run database updates manually.

STEP 3. CONFIGURING APPLICATION UPDATES

The **Configure proxy server to receive updates and connect to Kaspersky Security Network** window of the Configuration Wizard lets you configure a proxy server used with Kaspersky Security.

To configure a proxy server:

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.

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

STEP 4. COMPLETING APPLICATION CONFIGURATION

To stop the application configuring:

1. If you want Kaspersky Security Administration Console to start automatically after closing the Configuration Wizard, leave the **Start Administration Console** 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 Administration Console** check box was selected, Administration Console starts as soon as the Configuration Wizard closes.

RESTORING THE APPLICATION

If the application malfunctions (due to a damaged executable file or database, 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 log files are not altered 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 8.0 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 **Restore** window.

5. In the **Restoring** 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 8.0 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 **Removal** 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**.

CONTACTING THE TECHNICAL SUPPORT SERVICE

This section provides information about how to obtain technical support and the requirements for receiving help from Technical Support.

IN THIS SECTION:

HOW TO OBTAIN TECHNICAL SUPPORT

If you do not find a solution to your problem in the application documentation or in one of the sources of information about the application (see section "Sources of information about the application" on page 8), we recommend that you contact Kaspersky Lab's Technical Support Service. Technical Support specialists will answer your questions about installing and using the application.

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 telephone. This method allows you to consult with specialists from our Russian-language or international Technical Support.
- By sending a query from your Kaspersky Account on the Technical Support Service website. This method allows you to contact Technical Support specialists through a request form.

Technical support is only available to users who purchased a license for the application. No technical support is available to users of trial versions.

TECHNICAL SUPPORT BY PHONE

If an urgent issue arises, you can call specialists at Russian-speaking or international Technical Support (http://support.kaspersky.com/support/contacts).

Before contacting Technical Support, please read the support rules (http://support.kaspersky.com/support/rules). This will allow our specialists to help you more quickly.

OBTAINING TECHNICAL SUPPORT VIA MY KASPERSKY ACCOUNT

My Kaspersky Account is your personal area (https://my.kaspersky.com) on the Technical Support Service website.

To obtain access to My Kaspersky Account, you should go through the registration procedure on the registration page (https://my.kaspersky.com/registration). Enter your email address and a password to log in to My Kaspersky Account.

In My Kaspersky Account, you can perform the following actions:

- Contact Technical Support and the Virus Lab.
- Contact Technical Support without using email.
- Track the status of your requests in real time.
- View a detailed history of your Technical Support requests.
- Receive a copy of the key file if it is lost or deleted.

An email request to the Technical Support Service

You can send an online request to Technical Support in English, Russian, German, French, or Spanish.

In the fields of the online request form, specify the following data:

- Request type
- Application name and version number
- Request description
- Customer ID and password
- email address

A specialist from the Technical Support Service sends an answer to your question to your My Kaspersky Account and to the email address that you have specified in your online request.

Online request to the Virus Lab

Some requests must be sent to the Virus Lab instead of Technical Support.

You can send requests to the Virus Lab in the following cases:

- If you suspect that a file or website contains a virus, but Kaspersky Security does not detect any threat. Virus Lab specialists analyze the file or URL that you send. If they detect a previously unknown virus, they add a corresponding description to the database, which becomes available when Kaspersky Lab anti-virus applications are updated;
- If Kaspersky Security detects a virus in a file or website, but you are certain that this file or website is safe.

You can also send requests to the Virus Lab from the request form page (http://support.kaspersky.com/virlab/helpdesk.html) without being registered in Personal Cabinet. On this page, you do not have to specify the application activation code.

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 SharePoint.InfoCollector.exe utility, and to send it to Technical Support.

You can read a description of Info Collector and download the tool at: http://support.kaspersky.com/faq/?qid=208642392.

KASPERSKY LAB ZAO

Kaspersky Lab software is internationally renowned for its protection against viruses, malware, spam, network and hacker attacks, and other threats.

In 2008, Kaspersky Lab was rated among the world's top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab is the preferred developer of computer protection systems among home users in Russia, according to the COMCON survey "TGI-Russia 2009".

Kaspersky Lab was founded in Russia in 1997. Today, it is an international group of companies headquartered in Moscow with five regional divisions that manage the company's activity in Russia, Western and Eastern Europe, the Middle East, Africa, North and South America, Japan, China, and other countries in the Asia-Pacific region. The company employs more than 2000 qualified specialists.

Products. Kaspersky Lab's products provide protection for all systems—from home computers to large corporate networks.

The personal product range includes anti-virus applications for desktop, laptop, and pocket computers, and for smartphones and other mobile devices.

Kaspersky Lab delivers applications and services to protect workstations, file and web servers, mail gateways, and firewalls. Used in conjunction with Kaspersky Lab's centralized management system, these solutions ensure effective automated protection for companies and organizations against computer threats. Kaspersky Lab's products are certified by the major test laboratories, are compatible with the software of many suppliers of computer applications, and are optimized to run on many hardware platforms.

Kaspersky Lab's virus analysts work around the clock. Every day they uncover hundreds of new computer threats, create tools to detect and disinfect them, and include them in the databases used by Kaspersky Lab applications. *Kaspersky Lab's Anti-Virus database is updated hourly*, *and the Anti-Spam database – every five minutes*.

Technologies. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. It is no coincidence that many other developers use the Kaspersky Anti-Virus kernel in their products, including: SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Critical Path (Ireland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (France), NETGEAR (USA), Parallels (Russia), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Many of the company's innovative technologies are patented.

Achievements. Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. For example, in 2010 Kaspersky Anti-Virus received several top Advanced+ awards in a test administered by AV-Comparatives, a respected Austrian anti-virus laboratory. But Kaspersky Lab's main achievement is the loyalty of its users worldwide. The company's products and technologies protect more than 300 million users, and its corporate clients number more than 200,000.

Kaspersky Lab's website:	http://www.kaspersky.com
Virus encyclopedia:	http://www.securelist.com/
Virus Lab:	newvirus@kaspersky.com (only for sending probably infected files in archives)
	http://support.kaspersky.com/virlab/helpdesk.html?LANG=en
	(for queries addressed to virus analysts)
Kaspersky Lab's web forum:	http://forum.kaspersky.com

INFORMATION ON THE THIRD-PARTY CODE

Information about third-party code can be found in the file named legal_notices.txt and stored in the application installation folder.

TRADEMARK NOTICE

The registered trademarks and service marks are the property of their owners.

Microsoft, SharePoint, PowerShell, Windows, Windows Server, SQL Server, Internet Explorer и Windows Vista are trademarks of Microsoft Corporation registered in the USA and other countries.

Firefox, Mozilla is trademark of the Mozilla Foundation.

Google Chrome is a trademark owned by Google, Inc.

INDEX