# Kaspersky Security 9.0 for SharePoint Server


## Security Officer'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.



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: 9/10/2015



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

# CONTENTS

# ABOUT THIS GUIDE

This document is the Security Officer's Guide to Kaspersky Security 9.0 for SharePoint Server (hereinafter – Kaspersky Security).

This Guide is intended for professionals tasked with ensuring the security of confidential data, providing data leak prevention or preventing unauthorized access to data, and constantly monitoring the information security system and supporting its security hardware.

The Guide serves the following purposes:

- Help configure and use Kaspersky Security.
- Provide a readily search able source of information for questions related to operation of Kaspersky Security.
- References additional sources of information about the application and describes 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 7)**

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 9)**

This section describes the purpose and key features of the application and the specifics of user interaction with the application.

**Application usage scenarios (see page 12)**

This section describes usage scenarios for the main application features.

**Additional instructions (see page 57)**

This section lists instructions that help to configure application settings.

**Glossary (see page 50)**

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

### AO Kaspersky Lab

This section provides information about AO Kaspersky Lab.

### Information about third-party code (see page 55)

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

### Trademark notices (see page 56)

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. |
| **Example:**<br>... | Examples are given on a blue background under the heading "Example". |
| An *update* is...<br>The *Databases are outdated* event occurs. | The following items are italicized:<br>• new terms;<br>• status variations and application events. |
| Press **ENTER**.<br>Press **ALT**+**F4**. | Names of keyboard keys appear in bold and are capitalized.<br>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<br>The following message will appear:<br>`Specify the date in DD:MM:YY format.` | The following types of text content are set off with a special font:<br>• command line text;<br>• text of program messages output on the screen;<br>• 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 Anti-Virus 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, 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.ru/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.

Knowledge Base articles can answer questions relating to not only Kaspersky Anti-Virus 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 Security Officer's guide provides instructions on:

- Configuring Kaspersky Security settings.
- Using Data Leak Prevention functionality of Kaspersky 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.

# KASPERSKY SECURITY 9.0 FOR SHAREPOINT SERVER

Kaspersky Security 9.0 for SharePoint Server (hereinafter "the application") is designed to protect the SharePoint platform against viruses and other malware and to scan the content of web resources for unwanted content, protect personal data of users and confidential data of companies on SharePoint websites against data leaks.

Kaspersky Security 9.0 for SharePoint Server offers the following capabilities for the Security Officer:

- Detect data leaks in real time
- Block files containing confidential data at the time when they are uploaded to a SharePoint server
- Assign priorities to data leaks according to corporate security requirements
- Configure permissions to upload files to SharePoint for individual employees and organizational units
- Use statuses to monitor the processing of registered data leaks
- Save and archive data leak records
- Determine the exact location of files with confidential data on SharePoint
- Automatically send data leak notifications to email addresses
- Automatically or manually generate application reports and send them to email addresses

### IN THIS SECTION



## ABOUT THE SYSTEM OF ROLE-BASED ACCESS IN KASPERSKY SECURITY

Kaspersky Security supports the system of role-based user access for managing different functions of the application. User access to Kaspersky Security functions is granted depending on the user role.

Kaspersky Security supports the following roles:

- **Administrator**
- **Security officer**

The **Administrator** role is intended for installing and administering Kaspersky Security. The administrator has access privileges for managing keys, configuring and upgrading the application, functions of anti-virus protection of SharePoint servers and web content scanning.

The administrator assigns roles for managing different application functions, performs installation and initial configuration of Kaspersky Security for the security officer. During initial configuration, the administrator:

- Adds the active key of the application
- Connects the SharePoint server to Administration Console of Kaspersky Security on the computer of the security officer
- Activates the DLP Module component of Kaspersky Security, which is intended for use by the security officer

Prior to using Kaspersky Security, make sure that the administrator has performed initial configuration of the application.

The **Security Officer** role is intended to ensure the required level of corporate security on SharePoint websites. The Security Officer has access rights for managing protection of data against leaks.

The Security Officer can perform the following operations in the application:

- Create and modify the criteria of confidential data recognition on SharePoint web resources
- Configure methods of data leak detection and application actions upon leak detection
- Configure data leak notifications to email addresses
- View details of data leaks
- Archive old data leak entries and recover them from the archive
- Configure the settings of the search for files with confidential data on SharePoint websites;
- Generate data leak reports for different periods and configure the delivery of reports to email addresses
- View finished data leak reports

# ABOUT DATA LEAK PREVENTION

Kaspersky Security comprises the *DLP (Data Leak Prevention) Module* designed to protect data against leaks. The component monitors file uploads by users to SharePoint websites in real time and detects data leaks according to the following parameters:

- Type of data in the file and data contents;
- Name of the user transferring the file;
- SharePoint website to which the file is transferred.

You can configure these settings using categories (see section "Using categories. Assigning data to categories" on page 12) and policies (see section "Monitoring and preventing data leaks" on page 14) of the application.

If a user attempts to transfer a file containing confidential data (such as salary information of fellow employees) to a SharePoint website through which a leak may occur (such as a publicly accessible portal), the application registers this event as a data leak.

If national law requires notifying individuals that their network activity is being monitored, you must warn users about the operation of the DLP Module in advance.

You can configure the operations of Kaspersky Security as it registers data leaks. The application can perform the following operations automatically:

- Generate *incidents* (records documenting instances of corporate security violations)
- Assign priorities to incidents according to corporate security requirements
- Block file uploads to SharePoint
- Notify users and other officers about corporate security violations.

Information contained in incidents can be used to investigate corporate security violations.

# APPLICATION USAGE SCENARIOS

This section describes usage scenarios for the main application features. Scenarios offer recommendations on configuring Data Leak Prevention, managing incidents and reports, and contain links to helpful instructions.

### IN THIS SECTION



# USING CATEGORIES ASSIGNING DATA TO CATEGORIES

The application uses categories to monitor data leaks and search for information on SharePoint sites. Data categories contain criteria against which the application recognizes data matching the corporate information security restrictions on SharePoint sites.

In this application usage scenario, you will learn how to categorize data and use categories in the operation of Kaspersky Security. You can begin using the application by analyzing the data that needs to be protected against leaks and assigning such data to different categories.

Before performing this scenario, review the keywords used in Kaspersky Security:

- *Data category.* A set of data sharing a common feature or subject and meeting specific criteria (e.g., a set of words that come in a text in a specified order). The application uses data categories for recognizing information in files being uploaded and stored on SharePoint. The application allows using preset Kaspersky Lab data categories and creating custom data categories.

- *Table data.* Information organized in table format. When handling table data in Kaspersky Security, CSV (Comma Separated Values) files must be used.

- *Keywords.* Word, phrase, or sequence of characters that the application uses for recognizing data in files being uploaded and stored on SharePoint. Keywords can be added to a data category.

- *Kaspersky Lab categories* Predefined data categories developed by Kaspersky Lab specialists. Those categories can be used for monitoring data leaks and data search through files that are uploaded and stored on SharePoint. Categories can be updated when updating the application databases. A security officer cannot modify or delete predefined categories.

Task execution scenario:

1. Select data that matches a corporate security policy and divided them into groups based on common attributes (such as accounting records, personal data, or know-how). Highlight the criteria that set such data apart from other data (for example: data is stored in tables or names of new technologies or products are encountered in such data).

2. Based on these criteria and common attributes, select the types of categories for data recognition:

    - Use categories of table data to recognize information stored in tables (such as personal data of employees or payroll) (see section "Adding a category of table data" on page 28). You add table data to a category manually. The application recognizes data based on the number of table cell matches specified in the category settings.

- Use categories of keywords to recognize text information (such as information about technologies or processes of the company) (see section "Adding a category of keywords" on page 27). You add table keywords to a category manually. The application recognizes data based on keywords or expressions consisting of several keywords specified in the category settings.

- To recognize information based on popular categories (such as medical data, personal data, or banking data), use preset Kaspersky Lab categories (see section "About Kaspersky Lab data categories" on page 13).

You can use categories to monitor and prevent data leaks (see section "Monitoring and preventing data leaks" on page 14) and to search SharePoint websites for data (see section "Searching SharePoint websites for data" on page 15).

# ABOUT KASPERSKY LAB DATA CATEGORIES

*Kaspersky Lab categories* are preset categories developed by Kaspersky Lab. A category includes data subcategories (subordinated categories).

*Subcategory* is a nested, embedded data category included in a larger-scale category. Each subcategory describes a set of category data combined with a specific feature. For example, the "Magnetic stripe data" subcategory belongs to the "Payment cards" category.

You can change the contents of a category by selecting or excluding subcategories (see section "Changing the contents of a Kaspersky Lab category" on page 31). When a Kaspersky Lab data category is used, the application considers the data subcategories selected as part of this category. Subcategories excluded from the category scope are disregarded. For example, you can exclude from a category those subcategories for which the application generates false-positive incidents.

Kaspersky Lab categories are provided as part of the Kaspersky Security distribution kit. Categories can be updated when updating the application databases. The application records information about new Kaspersky Lab categories received during the update in the Windows Event Log. To receive information about how to add or edit preset Kaspersky Lab categories, you can set up automatic notification sending (see section "Configuring automatic notifications" on page 36). Notifications contain information about the number of new and modified categories and descriptions of the new categories.

*Table 2. Kaspersky Lab categories*

| CATEGORY NAME | CATEGORY DESCRIPTION |
|---|---|
| **Administrative documents** | This category allows detecting keywords and expressions used in administrative and regulating documents. Those include orders, notices, job descriptions, and applications from employees. Sets of data on administrative documents depend on the country in which they are used. |
| **Alcohol, tobacco, narcotic and psychoactive substances** | This category allows detecting keywords and expressions that may be directly or indirectly related to alcohol-containing beverages, tobacco goods, and narcotic, psychoactive and / or intoxicating substances. This may cover, e.g., ads or instructions on how to use or produce substances specified above. |
| **Discrimination** | This category allows detecting keywords and expressions that may infringe upon legitimate rights and interests of various groups of people. Any significant distinction of a person may become a cause for discrimination, such as sex, race, religious beliefs, sexual orientation, nationality, and occupation. |
| **Confidential documents** | This category allows detecting keywords and expressions used in confidential documents. Such documents include marks indicating their confidential nature: “For Internal Use Only”, “Confidential”, and “Not for External Distribution”. |
| **Medical data (UK)**<br>**Medical data (Germany)**<br>**Medical data (Russia)**<br>**Medical data (USA)**<br>**Medical data (France)** | These categories let you scan files for numbers of health insurance policies, patient case histories, diagnoses, and doctor's recommendations. The scope of data on pharmaceuticals, medical procedures, and social insurance details depend on the country in which the person receiving medical aid is resident. (Registered trademarks and service marks are the property of their respective owners.) |

| CATEGORY NAME | CATEGORY DESCRIPTION |
|---|---|
| **Violence** | This category allows detecting keywords and expressions that relate to the description of cruelty and violence. The category also allows detecting keywords and expressions that provoke actions constituting a menace to life and / or health (including actions of causing harm to one's own health and suicidal attempts). |
| **Negative emotional state** | This category allows detecting keywords and expressions that may indicate employees' depression or discontent. For example, employees may speak negatively of their managerial staff, colleagues, and customers, or they may express discontent with their job or salary. Such views may indicate a negative emotional condition of employees and a decrease of their working efficiency. |
| **Explicit language** | This category allows detecting rude and abusive words and expressions, as well as dirty language. |
| **Weapons and explosives** | This category allows detecting keywords and expressions that relate to the production and use of weapons, explosives, and pyrotechnics. This includes, e.g., descriptions of warfare, as well as historical, technical, and encyclopedic data related to weapons, explosives, and pyrotechnics. |
| **Personal data (UK)**<br>**Personal data (Germany)**<br>**Personal data (Russia)**<br>**Personal data (USA)** | Categories let you scan files for personal data based on which a person's identity or location can be determined (such as the date of birth, address of residence, passport or driver's license details, social security and social insurance numbers, bank card and account data and other information). The scope of personal data depends on the law of the country in which a person is resident. |
| **Payment cards** | This category lets you scan files for data protected under the international Payment Card Industry Data Security Standard (PCI DSS). The requirements of this standard apply to companies that work with international payment systems. These requirements protect personal details of payment card holders while they are processed, transmitted, and stored. This category helps to detect payment card and magnetic stripe data. |
| **HIPAA Federal Act (the USA)** | This category lets you scan files for data protected under the US HIPAA Act (The Health Insurance Portability and Accountability Act). This act is aimed at protecting the confidentiality of information about the physical and mental condition of patients. The requirements of this act apply to healthcare institutions and medical workers who transmit patient health information in electronic form. |
| **Federal Law No. 152 (Russia)** | This category allows scanning files for data protected by Russian Federal Law No. 152. This law is aimed at protecting personal data as it is being processed, stored or used. The requirements of the law apply to *personal data operators* (governmental agency, municipal agency, legal entity or individual that organizes or performs processing of personal data, and determines the objectives of personal data processing and the scope of personal data to be processed). These requirements govern activities involving collection, processing, storage, and transmission of personal data of citizens. |
| **Financial documents** | This category allows detecting keywords and expressions used in financial documents. Those include contracts, invoices, receipts, payrolls, and payment orders. Sets of data on financial documents depend on the country in which they are used. |
| **Erotica and pornography** | This category allows detecting keywords and expressions that relate to the sexual side of human relationships. This includes, e.g., descriptions of people's genitals, sexual intercourse or sexual perversions, self-pleasure. |

# MONITORING AND PREVENTING DATA LEAKS

You can track and prevent data leaks on SharePoint sites using the DLP function.

A *policy* is a way to specify data leak detection criteria for the application and configure its actions on leak detection. A policy contains a set of application settings for monitoring SharePoint websites for leaks of data belonging to a certain category. The application uses policies to monitor file uploads to SharePoint websites by users. If a user attempts to access data that is outside the scope of the user's job description, the application considers it a *policy violation*.

A policy is installed for a category of data. Several policies can be assigned for one category.

Task execution scenario:

Before completing this task, you are advised to create categories according to which the application will monitor and prevent data leaks (see section "Using categories. Assigning data to categories" on page 12).

1. Select the category whose data you want to monitor.

2. Define the data leak recognition criteria corresponding to the selected category: which users are not allowed to upload files to SharePoint, which users are allowed to upload files by way of an exclusion, and specify the websites to which users are not allowed to upload files.

3. Assign one or several policies for this category (see the section "New Policy Wizard" on page 34).

   In the policy settings, specify the users who are not allowed to transfer files with data matching the selected category.

The policy is active on the selected SharePoint sites from the time when it is created. The application scans file data and generates incidents when the policy is violated.

Select the **Block file** check box in the policy settings in order to prevent all kinds of data leaks. In this case, the user is unable to upload the file to SharePoint. The application sends an automatic policy violation notification to the user's email address. This option is recommended if the probability of data leaks during file uploads is high.

# SCANNED FILE FORMATS

To protect data against leakage, Kaspersky Security scans files uploaded to SharePoint for data of specific categories. The application determines the format of each file being scanned by analyzing its structure, which defines the way the file is stored or displayed on the screen. The extension of a file may not match its format. The application unpacks archived files down to the 64-th nesting level and scans all embedded objects. The file formats that the application handles are listed below.

*Table 3. Scanned file formats*

| FILE TYPE | FORMATS |
|---|---|
| Archives | 7Z; ARJ; BZ2; CAB; CPIO; DMG; EXE; GZ; ISO; JAR; OBD; RAR; RPM; TAR; TBZ2; ZIP |
| Databases | DB; DB3; DBF |
| Documents | AMI; DCA; DOC; DOCX; DOX; .DW5; FFT; FW3; JTD; JBW; JTT; HWP; IWP; JBW; JTD; JTT; KEY; M11; MAN; MANU; MNU; NUMBERS; ODT; PAGES; PDF; PUB; PW; PW1; PW2; QA; QA3; RFT; SAM; SDW; SXW; WPD; WRI; WS; WSD; WS2; WSx; XY |
| E-mail messages | EML; EMLX; MBOX; MBX; MHT; MSG; PST; OST; OFT |
| Presentations | ODP; ODS; PPT; PPTX; SXI; SDI; SDP |
| Tables | CSV; FW3; ODS; SX, SXC; SXS; WK; WK3; WK4; WKS; WPS; XLS; XLSB; XLSX |
| Text | CHM; DCA; EMF; HTM; HTML; ONETOC; RTF; SGML; TXT; XML; WMF |

The application does not monitor uploads of other file formats to SharePoint by users. If other file formats also contain any confidential information, advanced tools and techniques of data leakage control are advised to use along with the application.

# SEARCHING SHAREPOINT WEBSITES FOR DATA

Data search functionality lets you scan files on SharePoint sites for data belonging to specific categories.

You can use data search to perform the following operations:

- Detect all SharePoint sites that currently store files containing data that belongs to specific categories.
- Scan selected SharePoint sites for files containing data that belongs to specific categories. For example, you can receive information on files with employees' financial or personal data that are stored in improper locations.
- Use data categories to search SharePoint sites for specific files. For example, you can detect a file if its name and format are unknown but you know what type of data it may contain and on which SharePoint website it may be stored.

During data search, the load on SharePoint servers increases. To maintain a balanced load, the administrator can limit the list of SharePoint servers on which data search is available. If the **Status** column next to a running task displays the *No servers available* message, contact the administrator for a permission to run the task. The administrator modifies the DLP Module settings.

### Managing search tasks

The SharePoint site data search function is implemented in the form of search tasks (see section "Adding a search task" on page 26).

You can configure the following settings for each task:

- Scan type (full or incremental)
- Data categories according to which the search is performed
- SharePoint sites on which the search is performed
- Task run mode and schedule
- Application actions on detecting files that match the search conditions

  On detecting files, the application can create incidents and log event information in Windows Event Viewer.

You can add several search tasks to scan various SharePoint servers for files containing data that belongs to various categories. If necessary, you can edit the search task settings (see section "Editing search task settings" on page 30).

If data categories selected for running the search are modified while the search task is in progress (for example, certain keywords are removed or new table data is added), the application continues to search for files according to the modified data categories. The application does not re-scan the files that have been found.

The application searches for data in background mode. Regardless of the task run schedule, you can manually start or stop a search task at any time (see section "Starting and stopping a data search" on page 30).

The application does not scan system files during a search task.

The progress of the search task is displayed in the form of a progress bar. The progress bar shows the percentage ratio of files that have been scanned against the total number of files on the selected SharePoint servers.

### Data search optimization

During repeated runs of a task, the application can perform an *incremental scan*, i.e.,scan only files that have been modified since the previous task run (see the section "Features of incremental scanning" on page 17). Incremental scanning allows minimizing the task runtime and reducing the workload on the SharePoint server. You can enable the incremental scanning in the task settings (see the section "Enabling the incremental scanning" on page 24). If incremental scanning is disabled, the application scans all files that meet the search criteria.

### Processing search results

The application generates a report on search results after the task is completed (see section "Viewing search results" on page 45).

Each report contains a table with a list of files matching the search parameters. The report name is created automatically and matches the name of the task based on which it has been generated.

If necessary, you can save the report to view search results without opening Administration Console (see section "Saving search results" on page 48).

On the basis of search results, you can analyze the current data protection status on SharePoint and, if necessary, make changes to policies (see section "About Kaspersky Lab data categories" on page 13).

# FEATURES OF INCREMENTAL SCAN

*Incremental (partial) scan* is a type of file scan during which the application only scans files that have been modified since the previous scan. By default, the incremental scanning is enabled (see the section "Enabling the incremental scanning" on page 24). The application performs a full scan at the first task run; all further runs enable incremental scans. The application does not scan files that have not been modified. Modifying the scan task may cause the scan scope to include files that have not yet been scanned. The application performs a full scan of those files.

*Table 4. Dependency of the incremental scan on changes made to the scan task settings*

| SCAN SETTING | SETTING MODIFICATION | SCAN TYPE | FILES SCANNED BY THE APPLICATION |
|---|---|---|---|
| Data categories | No. No data categories have been modified in the task. | Incremental | Modified files only. |
| | Yes. A new data category (or multiple ones) has been added to the scan task. | Full and incremental | All files are scanned for presence of the specified new categories.<br>Modified files for presence of specified categories that have been used during the previous task run. |
| | Yes. The contents of a data category (or multiple ones) have been modified. | Incremental | Only modified files by updated categories. |
| Scanned websites | No. | Incremental | Modified files only. |
| | Yes. A new SharePoint website (or multiple websites) has been selected. | Full and incremental | All files located on new SharePoint websites.<br>Modified files on websites that have been scanned during the previous task run. |

# MANAGING INCIDENTS

An incident is a record about an application event associated with a possible data leak. Kaspersky Security generates incidents in the following cases:

- When a policy is violated
- While searching SharePoint for data

Each incident contains detailed information about incident-related files and users and the reason why the incident has been generated. This information is needed to analyze and investigate possible data leaks.

The incident workflow process is regulated by job descriptions of security officers and may vary depending on the incident workflow regulations adopted within an organization.

### Managing the incident workflow process

The incident workflow process can be managed as follows:

- Using incident statuses

  The incident status is information about the current incident status. The incident status can be changed at any time. Information about the incident status change and the author of changes is saved in the incident history.

  The application lets you change the status of several incidents at once (see section "Changing incident status" on page 32).

- Using comments

  Comments may contain information about the reasons for incident status changes and about an investigation of the circumstances under which the incident occurred.

Incident comments can be added while changing the incident status or viewing the incident history.

### Selecting incidents to manage

The application adds all incidents that are generated to the list of incidents in the **Incidents** node. You can change the appearance of the incident list by changing the incident information displayed in the table (see section "Changing incident details displayed in the table" on page 31).

The application automatically assigns *New* status to an incident when it is generated. New incidents available for processing can be displayed by refreshing the incident list (see section "Refreshing the list of incidents" on page 41).

You can use the incident filter to search for incidents according to specific criteria (such as incidents related to a specific user) (see the section "Searching for incidents using a filter" on page 41). You can use the search for similar incidents to handle similar incidents, i.e., those who share identical data (see the section "Searching for similar incidents" on page 42).

### Viewing incident details and processing incidents

You can start managing new incidents by viewing the incident details (see section "Viewing incident details" on page 42).

Incidents assigned for processing must have their status changed to *In progress*. If the company has several security officers, this will help them to coordinate their workflows.

To make a decision on an incident, you have to look at the context of the policy violation. The violation context is displayed in the incident details window. The violation context contains all text fragments that contain data indicating the violation. Keywords or table data are highlighted in red in each fragment. If the context of the violation is insufficient to make a decision on an incident, you can open the incident-related file on SharePoint.

When you point the mouse pointer on a text fragment that indicates a violation, a pop-up tip with the name of the *data subcategory* appears next to the pointer (see figure below). A subcategory is a nested, embedded data category included in a larger category. The subcategory name helps to define more accurately the area of the category to which data belongs.

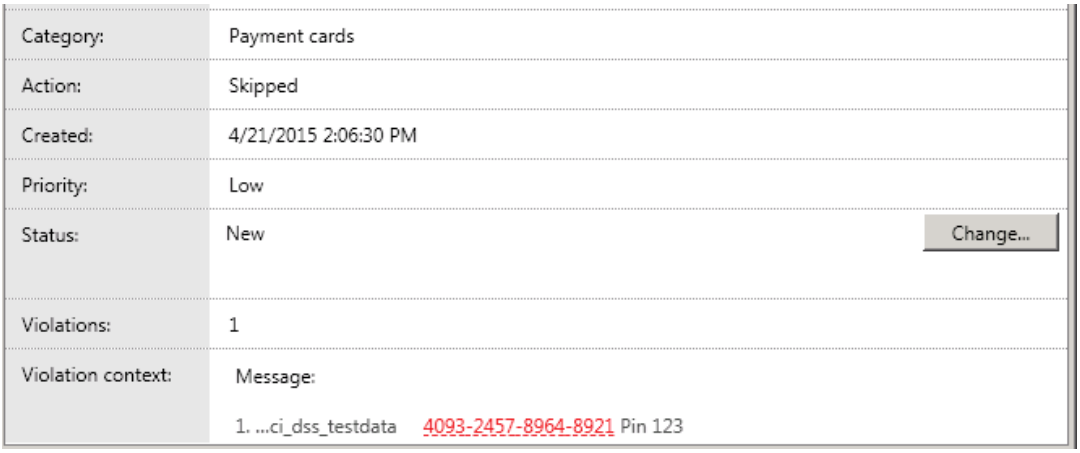


*Figure 1: The category name is displayed in a pop-up tip*

You can add the web address of the incident-related file to exclusions (see the section "Adding a file to exclusions by web address" on page 29). This helps you to reduce the number of false positive incidents generated when scanning template-based documents (such as uniform contracts or statements). The application adds the web address of a file to exclusions as follows:

- If the incident has been created due to a policy violation, the web address will be added to the policy's exclusions. The application will not control the uploading of files by users to that web address.
- If the incident has been created when running the search task, the web address will be added to the search task's exclusions. The application will not scan files located on that web address.

If the incident was generated while running a search task of Kaspersky Security 9.0 , you cannot add the file's web address to exclusions for the search task.

If you need to export incident details to create a service reference, you can copy the incident details to the clipboard (see the section "Copying incident details to the clipboard" on page 33).

### Finishing incident management

Following analysis of incident information, an incident can be assigned one of the following statuses:

- *Closed (processed)*, if incident processing has been completed.
- *Closed (false positive)*, if the policy violation was a false positive (for example, a mistake was made while configuring the policy).
- *Closed (not an incident)*, if the policy violation was admissible as an exclusion.
- *Closed (other)* in all other cases.

After finishing incident processing, you can remove them from the list of incidents by archiving them (see section "Archiving incidents" on page 23).

You are advised to perform archiving of incidents once the number of incidents exceeds 100,000. Kaspersky Security can be unstable when the number of incidents increases to 300,000.

### Recovering incidents

You can consult archived incidents, if necessary, by recovering incidents (see section "Restoring incidents from the archive" on page 24). The application automatically assigns *Archival* status to all restored incidents.

After you finish processing these incidents, you can remove them from the list (see section "Deleting archived incidents" on page 48).

# GENERATING APPLICATION REPORTS

Information on the operation of the application and the status of Data Leak Prevention can be saved in reports. Reports are generated on the basis of information stored in the database. You can generate a report manually or automatically (according to schedule).

You can use quick reports to generate reports manually (see section "Generating a quick report" on page 47).

You can use report creation tasks to generate reports automatically (see section "Adding a report creation task" on page 26). Report generation tasks are started according to the schedule configured in task settings. If necessary, you can generate a report at any time without waiting for a scheduled task to start (see section "Starting a report generation task" on page 29).

### Selecting the report type

You can select the report type depending on the type of information you need to gather:

- To gather full information on the results of application operation and the status of Data Leak Prevention during a specific period, generate a report on policy-related incidents. The report contains information about incidents related to the selected categories and policies (see section "Configuring settings of the report on policy-related incidents" on page 36).

- To gather information about policy violations by specific users, generate a “user statistics” report. The report contains information about incidents related to the selected users (see section "Configuring the report on users" on page 37).

  You can use the report to analyze the frequency of policy violations by users. For example, if a user has repeatedly violated the same policy, you have to notify the user's manager.

- To check if the application is running properly, generate a system KPI (Key Performance Indicators) report. The report contains information on the key performance indicators of the application (see section "Configuring the system KPI report" on page 38).

  You can track changes in the operation of the application based on this report. For example, if the application has not scanned a large number of files, this may indicate a need to modify policy settings.

- To check if policies are configured correctly, generate an “incident status report”. The report contains information about incidents related to the selected data categories (see section "Searching SharePoint websites for data" on page 15).

  This report lets you analyze relationships between policy violations and reasons for closing incidents. For example, if policy-related incidents are closed as false positives, this may indicate a need to change the policy settings.

When generating a “report on policy-related incidents” or a “user statistics report”, the application factors in the incidents restored from the archive.

### Managing reports

The application adds all reports that have been generated to the list of reports in the **View and create reports** section in the **Reports** node. The following information is displayed for each report:

- Name.
- Creation date and time.
- The reporting period.
- Report type.

This information helps you to find reports that you want to view. If you generate a quick report, the application automatically opens the generated report in the window of the default browser.

If necessary, you can save the generated reports to manage them without opening Administration Console (see section "Saving reports" on page 47).

# ASSESSING THE STATUS OF DATA PROTECTION

The status of data protection has to be assessed constantly in order to maintain the proper level of data security on SharePoint websites. Information about data protection is refreshed in real time in the **Data Leak Prevention** node (see section "**Viewing protection status details**" on page 46).

The status of data protection can be assessed using the following criteria:

- Status of the DLP Module, errors in the operation of the Module;

  If the DLP Module operates with errors, this decreases the level of protection. If the DLP Module is disabled, the application does not scan files that are uploaded by users to SharePoint.

- Statistics on opened incidents;

  This information helps to evaluate the volume of incidents processed so far and plan further incident processing.

- Statistics on closed incidents;

  This information helps to analyze the reasons why incidents have been closed. Analysis results help to detect weak spots in computer protection and modify policy settings accordingly.

- Statistics on files uploaded to SharePoint.

  This information helps to monitor and evaluate application performance.

You can set up the automatic delivery of notifications about changes in the protection status to email addresses (see the section "Configuring automatic notifications" on page 36).

# ADDITIONAL INSTRUCTIONS

This section lists instructions that help to configure application settings.

## IN THIS SECTION

# ARCHIVING INCIDENTS

*Incident archiving* is a process of moving closed incidents to an archive in secure format.

Incident archiving reduces the size of the SQL database and the list of incidents displayed in Administration Console.

*To launch the Incident Archiving Wizard:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Incidents** node.
3. Select closed incidents to be moved to the archive.
4. Click the **Archive** button in the workspace of the node.

The application launches the Incident Archiving Wizard.

The interface of the Incident Archiving Wizard consists of a sequence of windows (steps). Use the **Back** and **Next** buttons to navigate the windows of the Wizard. To close the Wizard after it finishes, click the **Finish** button. To exit the Wizard at any step, click the **Cancel** button.

## Step 1. Starting the Wizard. Selecting incidents to archive

The first window of the Wizard shows information about incidents to be archived. You can archive incidents with the *Closed* status only.

In the **Path to file** field, specify the full path to the archive in which the application will save incidents. If you do not specify the name of an archive, the Incident Archiving Wizard creates a new incident archive. The archive name is assigned automatically and contains the date of creation of the earliest incident in the archive and the date of creation of the most recent incident in the archive. The application uses the dates when incidents were created on the server.

You cannot archive incidents with *New* or *In progress* status or incidents previously recovered from the archive.

### Step 2. Creating an archive with incidents

At this step the Wizard performs incident archiving. The incident archiving process is accompanied by a progress bar. Once incident archiving has been completed, the Wizard automatically proceeds to the next step.

### Step 3. Exiting the Wizard

At this step the Wizard announces that the incident archiving process has been completed and shows information on the number of incidents archived. If errors were encountered during the incident archiving process, the Wizard displays information about the incidents that could not be archived.

The following archiving process information is stored in the incident history:

- Archive name
- Date and time of the archiving process
- Name of the user that performed archiving

Incidents added to the archive are removed from the SQL database and the list of incidents in the **Incidents** node.

# ENABLING THE INCREMENTAL SCANNING

*To enable the incremental scanning:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Search** node.
3. In the list of tasks in the **Search tasks** section, select the task whose settings you want to edit and click the **Change** button.

   The **Task settings** window opens.
4. On the **General** tab, select the **Scan modified files only** check box.

   During repeated runs of the task, the application will scan files that have been modified since the previous task run.
5. Click **OK** to save changes.

Editing the search task settings affects the incremental scanning (see the section "Features of incremental scanning" on page 17).

# RESTORING INCIDENTS FROM THE ARCHIVE

*Incident recovery* is a process of copying incidents from the archive to the SQL database.

You can recover incidents when you need to view the details of incidents that had been processed a long time ago.

*To launch the Incident Recovery Wizard:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Incidents** node.
3. Click the **Restore** button in the workspace of the node.

The application starts the Incident Recovery Wizard.

The interface of the Incident Recovery Wizard consists of a sequence of windows (steps). Use the **Back** and **Next** buttons to navigate the windows of the Wizard. To close the Wizard after it finishes, click the **Finish** button. To exit the Wizard at any step, click the **Cancel** button.

### Step 1. Starting the Wizard. Selecting incidents to recover

In the first window of the Wizard, select the incidents that you want to recover.

In the **For period** field, specify the period during which the incidents you need were generated. In the **Path to file** field, specify the full path to the file of the incidents archive from which the application will restore the incidents.

### Step 2. Recovering incidents

At this step the Wizard performs incident recovery. The process of incident recovery from the archive is displayed in the Wizard window using a progress bar. Once incident recovery has been completed, the Wizard automatically proceeds to the next step.

### Step 3. Exiting the Wizard

At this step the Wizard announces that the incident recovery process has been completed and shows information on the number of incidents recovered. If errors were encountered during the incident recovery process, the Wizard displays information about the incidents that could not be recovered.

Recovered incidents cannot be archived or recovered again. It is impossible to change the status of recovered incidents.

All recovered incidents are displayed in the common list of incidents in the **Incidents** node. *Archived* status is added to the status of recovered incidents.

# SELECTING CATEGORIES FOR GENERATING INCIDENT STATISTICS

*To select categories to be included in the statistics chart:*

1. Open Administration Console.
2. In the tree of Administration Console nodes, select the **Data Leak Prevention** node.
3. Perform one of the following steps:
   - To generate a chart on opened incidents, click the **Select categories** button in the **Opened incidents** section.
   - To generate a chart on closed incidents, click the **Select categories** button in the **Statistics** section.

   The **List of categories** window opens.

4. In the **List of categories** window, select categories of data to be included in statistics.

   The application generates incident statistics based on the categories selected.

   If the **All categories** check box is selected, when new categories are added the information about incidents related to new categories is automatically added to the statistics chart.

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

Data on incidents created according to the selected categories is reflected in the chart.

# ADDING A SEARCH TASK

*To add a search task:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Search** node.
3. In the **Search tasks** section, click the **Create** button.

   The **Task settings** window opens.
4. On the **General** tab, in the **Task name** field specify the task name.
5. If necessary, select the **Scan modified files only** check box.

   During repeated runs of the task, the application will scan files that have been modified since the previous task run.
6. If necessary, select the **Create incidents** and **Log events in Windows Event Viewer** check boxes.

   On detecting files that contain data of the specified categories, the application creates an incident for each file and logs file detection information in Windows Event Viewer.
7. On the **Categories** tab, select the check boxes next to data categories for which the application should find matches on SharePoint websites.
8. On the **Schedule** tab, select the task run mode and configure the task run schedule.
9. On the **Search scope** tab, select the check boxes next to SharePoint websites on which the application will search for files.
10. If necessary, click the **Add exclusion** button to configure exclusions for websites**.**

    The application will not scan files located on the web addresses that you have specified.
11. Click **OK** to finish creating the task.

The new task is displayed in the table of tasks in the **Search tasks** section. You can start a task manually after creating it. If you have configured a task run schedule, the application runs a search for data at the specified time on the specified day.

# ADDING A REPORT GENERATION TASK

*To add a report generation task:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Reports** node.

3. In the **Report creation tasks** section, click the **New task** button.
4. In the drop-down list that opens, select the type of report to be generated.

   The **Task settings** window opens.
5. In the window that opens, configure the settings of the report generation task.
6. Click **OK** to add the task.

The new task is displayed in the list of tasks in the **Report creation tasks** section. The application starts the report generation task automatically according to the schedule configured in the task settings.

# ADDING A CATEGORY OF KEYWORDS

A *keyword* is a word, phrase, or set of characters using which the application identifies data on SharePoint sites. To search SharePoint sites for data using keywords, you have to add keywords to a category. A category can contain a single keyword or an expression consisting of several keywords.

*To add a category of keywords:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Categories and policies** node.
3. In the workspace of the node, click the **New category** button and select the **Keywords** option in the list of category types that opens.

   The **Category settings** window opens. This window lets you add keywords to a category and specify the category name.
4. In the entry field, type the keywords to be included in the category.

   A keyword is a word or word combination enclosed in quotation marks. Use the "!" character at the beginning of the keyword to make it case-sensitive. Keywords can be combined into expressions by using such operators as AND, OR, NEAR(n), and ONEAR(n). Use round brackets to specify the order in which the operators should be applied.

   The OR operator is applied automatically to keywords typed in the entry field beginning with a new line. The application detects files whose text includes keywords consisting of one or more lines of the category.

**Example:**

The category contains the following expression consisting of keywords:

"security" AND ("!Kaspersky Lab" NEAR(5) "program code")

The application detects files whose content matches the following criteria:

- They include words and word combinations "security", "Kaspersky Lab", and "program code".
- The words "Kaspersky Lab" begin with upper-case letters.
- The word combination "program code" is used before or after the word combination "Kaspersky Lab" with five or fewer words between them.

  For example: "...protect the program code of the application against hacking. At the conference, Kaspersky Lab will showcase an improved version of the product that makes networking more secure".

Detailed information on adding a category of keywords is available via the **Help on adding keywords** link in the **Category settings** window.

5. Specify the category name in the **Name** field.
6. Specify additional information pertaining to data included in the category in the **Comments** field.
7. Click **OK**.

   The new category is added to the list of categories in the **Categories and policies** node.

You can use a category to search SharePoint sites for data and monitor data leaks.

# ADDING A CATEGORY OF TABLE DATA

*Table data* describes information that is arranged in the form of tables. A common method of storing table data is a CSV (Comma Separated Values) file. Lines in CSV files correspond to table rows. Table rows in CSV files are separated using a special character known as the *column separator*. For example, a semicolon can be used to separate columns in a CSV files.

The application uses categories of table data to search for table data on SharePoint sites. The category contains the path to a CSV file with table data that needs to be monitored to prevent potential leaks, and also data search criteria.

A CSV file can be opened in such applications as Notepad, WordPad, or Microsoft Excel.

*To add a category of table data:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Categories and policies** node.
3. In the workspace of the node, click the **New category** button and select the **Keywords** option in the list of category types that opens.

   The **Category settings** window opens. This window lets you add table data, configure data search settings, and specify the category name.
4. In the **Path to file** field, enter the full path to the location of the CSV file with table data to be added to the category.

   For the category of table data to work properly, the CSV file must be saved using UTF-8 encoding.
5. In the **Column separator** drop-down list, select the symbol to be used as the column separator in the CSV file that you are uploading.

   By default, the comma is used to separate columns.
6. Configure the match level for table data.

   The *match level* is the minimum number of cells with table data whose content matches data in SharePoint files. The number of cells is defined as the number of unique intersections between columns and rows in the table.

   - In the **Threshold value of rows** spin box, specify the number of table rows.

     By default, the application detects files with data present in any two table rows.
   - In the **Threshold value of columns** spin box, specify the number of table columns.

     By default, the application detects files with data present in any two table columns.

   Detailed information on adding a category of table data is available via the **Help on configuring the match level** link in the **Category settings** window.

7. Specify the category name in the **Name** field.
8. Specify additional information pertaining to data included in the category in the **Comments** field.
9. Click **OK**.

   This opens a window showing the progress of table data being loaded into a category.

   When table data is added to a category, the first row in the CSV file is ignored (it is presumed that the first row contains table header data).

   If an error is encountered while table data is being added to a category, the application shows a notification with the number of the table row that caused the error.

   The new category is added to the list of categories in the **Categories and policies** node.

You can use a category to search SharePoint sites for data and monitor data leaks.

# ADDING A FILE TO EXCLUSIONS BY WEB ADDRESS

*To add an incident-related file to exclusions by its web address:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Incidents** node.
3. In the list of incidents, select one for which the related file should be added to exclusions.
4. Click the **View** button.

   The **Incident details** window opens.
5. In the **File** row, click the **Actions** button, and in the drop-down list that opens select **Add to exclusions**.

   The application adds the web address of the incident-related file to exclusions as follows:

   - If the incident was created due to a policy violation, the web address will be added to the policy's exclusions. The application will not control the uploading of files by users to that web address.
   - If the incident was created when running the search task, the web address will be added to the search task's exclusions. The application will not scan files located on that web address.

   If adding the web address to exclusions has failed (e.g., due to the policy or search task that had been removed), the application displays an error message.
6. Click **OK** to save changes.

# STARTING A REPORT GENERATION TASK

*To start a report generation task:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Reports** node.
3. Select the task to be started in the **Report creation tasks** section.
4. Click the **Start task** button.

The application generates the report according to the configured task settings. The report appears in the list of reports in the **View and create reports** section.

# STARTING AND STOPPING A DATA SEARCH

*To start or stop a search task manually:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Search** node.
3. In the list of tasks, select the search task that you want to start or stop.
4. Perform one of the following steps:
   - To start a search task, click the **Start** button.

     The application starts the data search on SharePoint websites.
   - To stop the search task, click the **Stop** button.

     The application stops running the task. After stopping the task, the application generates a report with information on files found before the task was stopped. The report is displayed in the **Search results** section.

If the **Status** column next to a running task displays the *No servers available* message, contact the administrator for a permission to run the task. The administrator modifies the DLP Module settings.

# EDITING SEARCH TASK SETTINGS

*To edit search task settings:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Search** node.
3. In the list of tasks in the **Search tasks** section, select the task whose settings you want to edit and click the **Change** button.

   The **Task settings** window opens.
4. Make changes to the task settings in the window that opens.
5. Click **OK** to save changes.

Editing the search task settings affects the incremental scanning (see the section "Features of incremental scanning" on page 17).

# EDITING REPORT GENERATION TASK SETTINGS

*To edit the settings of a report generation task:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Reports** node.
3. In the **Report creation tasks** section, select a task and click **Edit**.

   The **Task settings** window opens.

4. Make changes to the task settings.
5. Click **OK** to save changes.

## EDITING A CATEGORY

*To edit a category:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Categories and policies** node.
3. In the list of categories, select the category whose settings you want to edit and click the **Settings** button.

   The category settings window opens.
4. Edit the category settings in the window that opens.
5. Click **OK** to save changes.

## CHANGING INCIDENT DETAILS DISPLAYED IN THE TABLE

*To change incident details displayed in the table:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Incidents** node.
3. In the **List of incidents** section, click the **Select columns** button.

   The **Select columns to display** section opens.
4. In the section, select check boxes opposite those incident details that you want displayed in the table.

Table changes are applied as soon as you select or clear a check box. Incident details next to which the icon  appears are always displayed in the table.

## CHANGING THE CONTENTS OF A KASPERSKY LAB CATEGORY

*To change the contents of a Kaspersky Lab category:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Categories and policies** node.
3. In the list of categories, select the Kaspersky Lab category in which you need to change the contents and click the **Settings** button.

   The category settings window opens.
4. In the **Subcategories** section, select the check boxes next to the data subcategories that you need to keep in this category.
5. Click **OK** to save changes.

# CHANGING INCIDENT STATUS

*Incident status* is information about the current incident status. You can change the incident status based on the results of incident processing. Incident statuses are used when generating application reports. The incident status can be changed either in the list of incidents or in the incident details window.

*To change the incident status:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Incidents** node.
3. In the list of incidents, select an incident whose status you want to change.

   You can select one or several incidents in the list.
4. Click the **Change status** button and select **Selected incidents** in the list that opens.

   You can change the status of all incidents in the list. To do so, select the **All incidents** option in the **All incidents** drop-down list.
5. In the **Change status** window that opens, in the **Status** list select the status that you want to assign to the incident.
6. If you need to specify the reason for the status change or other information pertaining to incident processing, add it in the **Comments** field.
7. Click **OK** to save changes.

The new incident status is displayed in the **Status** column of the incidents list in the **Incidents** node. Information about the status change and the author of changes is saved in the incident history.

You can change the status of an incident in the **Incident details** window by clicking the **Change** button.

# USING OPERATORS IN EXPRESSIONS

A keyword is a word, phrase, or sequence of characters that the application needs in order to recognize confidential data in text.

Words and phrases that have been specified as keywords and put into quotes, can be separated with whitespaces and other symbols (for example, "#", "%", "+", "@", "&", and punctuation symbols). Keywords can be combined into expressions by using such operators as AND, OR, NEAR(n), and ONEAR(n) (see table below).

*Table 5. Using operators in expressions*

| OPERATOR | DESCRIPTION OF USE | RESULT |
|---|---|---|
| ! | The "!" character is used at the beginning of a keyword to make it case-sensitive.<br>If the keyword consists of several words, the case operator applies to each word included in the keyword. For example, "!Kaspersky Lab". | The application detects files whose text includes the "Kaspersky Lab" keyword beginning with upper-case letters. Files containing this keyword in lower-case (such as "kaspersky lab") are skipped. |
| AND | Use the AND operator to detect two or more keywords included in the text at the same time. For example, "anti-virus" AND "security".<br>The order in which the keywords are enumerated does not affect the search. | The application detects files whose text includes the words "anti-virus" and "security" at the same time. Files containing only one of these words are skipped. |

| OPERATOR | DESCRIPTION OF USE | RESULT |
|---|---|---|
| OR | Use the OR operator to detect one of the keywords or several keywords in the text. For example, "security" OR "computer protection".<br>The OR operator is applied automatically to keywords typed in the entry field beginning with a new line. | The application detects files in which the text includes the word "security" or the word combination "computer security", or both. |
| NEAR(n) | The NEAR operator is used to detect several keywords separated by several other words in text. Specify the number of words separating the keywords in brackets. For example, "security" NEAR(6) "system".<br>The order in which keywords have been entered is disregarded during the search. | The application detects files in whose text the word "security" appears before or after the word "system" with six or fewer words between them. |

Use several operators to create complex expressions from keywords. Use round brackets to specify the order in which the operators should be applied.

**Example:**

The category contains the following expression consisting of keywords:

"security" AND ("!Kaspersky Lab" NEAR(5) "program code")

The application detects files whose content matches the following criteria:

- They include words and word combinations "security", "Kaspersky Lab", and "program code".
- The words "Kaspersky Lab" begin with upper-case letters.
- The word combination "program code" is used before or after the word combination "Kaspersky Lab" with five or fewer words between them.

For example: "...protect the program code of the application against hacking. At the conference, Kaspersky Lab will showcase an improved version of the product that makes networking more secure".

The search for expressions “term1” NEAR(n) (“term2” AND “term3”) and “term1” NEAR(n) (“term2” NEAR(m) “term3”) is not supported. When the application searches for data using these type of expressions, uncertainty arises when the brackets are removed.

# COPYING INCIDENT DETAILS TO THE CLIPBOARD

*To copy the incident details to the clipboard:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Incidents** node.
3. In the list of incidents, select the one of which you need to copy the details.
4. Click the **View** button.

   The **Incident details** window opens.
5. In the **File** field, click the **Actions** button, and in the drop-down list select **Copy data to clipboard**.

The application copies the incident details and processing history to the clipboard. The order and set of details being copied are the same as those displayed in the application window.

To continue handling the incident, you can paste the clipboard's contents to a text editor (such as Notepad or Microsoft Word).

# NEW POLICY WIZARD

A *policy* is a way to specify data leak detection criteria for the application and configure its actions on leak detection. A policy contains a set of application settings for monitoring SharePoint sites for leaks of data belonging to a certain category. Initial configuration of policy settings is performed with the help of the Policy Wizard.

- *To launch the Policy Wizard:*

  1. Open Administration Console.
  2. In the Administration Console tree of nodes, select the **Categories and policies** node.
  3. Select the data category for which you want to configure a policy.
  4. Click the **New policy** button.

  The application starts the Policy Wizard.

The interface of the Policy Wizard consists of a sequence of windows (steps). Use the **Back** and **Next** buttons to navigate the windows of the Wizard. To close the Wizard after it finishes, click the **Finish** button. To exit the Wizard at any step, click the **Cancel** button.

### STEPS OF THE WIZARD



# STEP 1. POLICY RATIONALE AND STATUS

At this step, you can change the policy status and specify the rationale for creating it.

- *To change the policy status,*

  Select the **Activate policy** check box.

When the wizard finishes, the application starts monitoring file uploads to SharePoint sites according to the settings configured in the policy.

- *To specify a rationale for a policy,*

  in the **Link to guidance document** field, specify the paragraph of the regulatory document that governs data confidentiality practices at the company.

A policy rationale is required to coordinate the efforts of several security officers working at the same company.

Specify the name of the policy being created in the **Policy name** entry field. If the entry field has a red outline, this means that a policy with this name already exists.

# STEP 2. CONFIGURING PERMISSIONS TO TRANSFER FILES

At this step, you can configure permissions for file transfer to SharePoint sites by users.

*To configure permissions for file transfers by users:*

1. In the **Policy applies to** list, select one of the following methods to apply the policy:
   - **All Active Directory users**
   - **Selected Active Directory users**

     The application uses Active Directory accounts to monitor user activity. Creating and managing Active Directory groups is the job of the company's system administrator. The  and  buttons are designed to add and remove user accounts to which a policy applies.
2. To specify users to be excluded from the scope of the policy, add their accounts to the **Exclude the following users from policy** list.

   Exclusions always have priority over permissions for file transfers by users. After a user account has been added to the exclusions list, the application stops monitoring this user's attempts to transfer files to SharePoint.

# STEP 3. SELECTING PROTECTED SHAREPOINT SITES

At this step, you can configure the control scope of the policy by specifying SharePoint websites for which the application will monitor file transfers.

*To configure the control scope:*

1. Select the check boxes next to SharePoint websites or use the **Select child items** and **Deselect child items** buttons to select the check boxes automatically.

   The application will control the uploading of files to the selected websites.
2. Configure exclusions from the control scope:

   a. Click the **Add exclusion** button.

      This opens the **Web address** window.

   b. In the window that opens, specify a web address and click **OK**.

The web address appears on the list of exclusions. The application will not control the uploading of files by users to that web address.

# STEP 4. ACTIONS UPON POLICY VIOLATION

A *policy violation* means user's actions leading to a violation of the conditions applied to the storage of confidential information on SharePoint websites. The user violates a policy by uploading policy-protected category data to SharePoint.

*To configure application operations upon a policy violation:*

1. Select the **Block file upload to SharePoint** check point to prevent leaks of data belonging to the specified categories.

   If the application detects data belonging to several categories while scanning a file, the file is blocked if at least one policy is configured to block data.

   If this check box is cleared, the application does not block file transfers to SharePoint but creates incidents when the policy is violated.
2. In the **Create incidents with priority** drop-down list, select the priority that the application will assign to incidents upon a policy violation.

3. If necessary, select the **Attach file to incident details** check box to view the file when managing the incident.
4. If necessary, select the **Record event to Windows Event Viewer** check box to save information about policy violations centrally and use it when resolving errors in the future.

   When a policy violation event is saved in Windows Event Viewer, it is assigned code 16000. Each record contains the incident number and incident information.
5. In the **Send notifications by email** list, select check boxes opposite the names of employees to be notified about policy violations. Select the **Additional** check box to enter email addresses in the entry field separated with a semicolon.

   In the event of a policy violation, the application sends notifications to these addresses.
6. Click **Finish** to close the New Policy Wizard.

A policy is assigned for a category of data. You can view the list of policies assigned for a category by clicking the  button. You can minimize the list of policies by clicking the button  . Policy lists are minimized automatically when you switch to another node of Administration Console.

# CONFIGURING AUTOMATIC NOTIFICATIONS

*To define the notification sending settings:*

1. Open Administration Console.
2. In the tree of Administration Console nodes, select the **Data Leak Prevention** node.
3. In the **DLP Module status** section, click the **Configure notifications** button.

   The **Notification settings** window opens.
4. In the entry field, specify the email addresses to which notifications should be sent. Use a semicolon to separate email addresses in the entry field.

   The application uses the specified addresses to send notifications of new incidents and the status of the DLP Module, as well as ready reports.
5. If necessary, select the **Notify when adding Kaspersky Lab categories** check box.

   The application sends automatic notifications of Kaspersky Lab categories that have been added or modified.
6. Click **OK** to save changes and close the window.

# CONFIGURING SETTINGS OF THE REPORT ON POLICY-RELATED INCIDENTS

*To configure the settings of the report on policy-related incidents:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Reports** node.
3. Configure a detailed report generation task or a quick detailed report:
   - To configure an existing detailed report generation task, select a task in the **Report creation tasks** section and click the **Change** button.

- To configure a quick detailed report, in the **View and create reports** section click the **New report** button and select **Policy-related incidents**.

  The report settings window opens.

4. Make changes to the report settings.
5. Click **OK**.

You can configure the settings of a detailed report as follows:

- Select incidents for the report on policies and categories.

  When you select a category, all policies configured for the category are selected automatically.

- Select incidents associated with specific users for the report.

  You can select individual users or groups of Active Directory users, anonymous users, or users without Active Directory accounts.

- Select incidents with specific statuses for the report.
- Configure the order for displaying incidents in the report.

  The application can group report incidents with the same information in the order that you specify.

- Specify the reporting period.

  If you create a quick report, you can specify any reporting period. If you configure a report task, the reporting period depends on the task schedule. For example, if you configured the task to run weekly, the report is generated for the past week.

- Configure the task launch schedule.

  The application generates reports automatically according to this schedule. If necessary, you can disable automatic launch of tasks.

- Configure automatic delivery of the report via email.

  If necessary, you can specify additional email addresses in the entry field, separating them with a semicolon. The application automatically sends the generated report to these addresses.

# CONFIGURING THE REPORT ON USERS

*To configure the settings of the report on users:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Reports** node.
3. Configure a task to generate a report on policies and incidents or a quick report on policies and incidents:

   - To configure an existing task to generate a report on policies and incidents, select a task in the **Report creation tasks** section and click the **Change** button.

   - To configure a quick report on policies and incidents, in the **View and create reports** section click the **New report** button and select **Incident status statistics**.

     The report settings window opens.

4. Make changes to the report settings.
5. Click **OK**.

You can configure the settings of a report on users as follows:

- Select users to be included in the report.

  You can select individual users or groups of Active Directory users, anonymous users, or users without Active Directory accounts. For users whose Active Directory accounts could not be determined, the SharePoint account may be displayed (for example: `SharePoint\Kaspersky`).

- Select incidents for the report on categories.

  The application displays the number of violations related to the selected data categories for each user.

- Select incidents for the report on statuses.

- Configure the order for displaying user information in the report.

  The application can group information about users who committed the same violations in the order that you specify.

- Specify the reporting period.

  If you create a quick report, you can specify any reporting period. If you configure a report task, the reporting period depends on the task schedule. For example, if you configured the task to run weekly, the report is generated for the past week.

- Configure the task launch schedule.

  The application generates reports automatically according to this schedule. If necessary, you can disable automatic launch of tasks.

- Configure automatic delivery of the report via email.

  If necessary, you can specify additional email addresses in the entry field, separating them with a semicolon. The application sends the generated report to these addresses.

# CONFIGURING THE SYSTEM KPI REPORT

*To configure the settings of the system KPI report:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Reports** node.
3. Configure a system KPI report task or a quick system KPI report:

   - To configure an existing system KPI report task, select a task in the **Report creation tasks** section and click the **Change** button.

   - To configure a quick system KPI report, in the **View and create reports** section click the **New report** button and select **System KPI**.

     The report settings window opens.

4. Make changes to the report settings.
5. Click **OK**.

You can configure the system KPI report settings as follows:

- Specify the reporting period.

  If you create the report manually, you can specify any reporting period. If the report is created automatically, the reporting period depends on the task run schedule. For example, if you configured the task to run weekly, the report is generated for the past week.

- Configure the task launch schedule.

  The application generates reports automatically according to this schedule. If necessary, you can disable automatic launch of tasks.

- Configure automatic delivery of the report via email.

  If necessary, you can specify additional email addresses in the entry field, separating them with a semicolon.

# CONFIGURING SETTINGS OF THE INCIDENT STATUS REPORT

*To configure the settings of the incident status report:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the Reports node.
3. Configure a task to generate a report on policies and incidents or a quick report on policies and incidents:
   - To configure an existing task to generate a report on policies and incidents, select a task in the **Report creation tasks** section and click the **Change** button.
   - To configure a quick report on policies and incidents, in the **View and create reports** section click the **New report** button and select **Incident status statistics**.

     The report settings window opens.
4. Make changes to the report settings.
5. Click **OK**.

You can configure the settings of a report on policies and incidents as follows:

- Select incidents for the report on categories.

  The application selects incidents with *Closed* status for the report. Incidents with other statuses will not be included in the report. For each incident related to the selected category, the policy and the reason of incident closing will be specified in the report.

- Specify the reporting period.

  If you create a quick report, you can specify any reporting period. If you configure a report task, the reporting period depends on the task schedule. For example, if you configured the task to run weekly, the report is generated for the past week.

- Configure the task launch schedule.

  The application generates reports automatically according to this schedule. If necessary, you can disable automatic launch of tasks.

- Configure automatic delivery of the report via email.

  If necessary, you can specify additional email addresses in the entry field, separating them with a semicolon. The application sends the generated report to these addresses.

# CONFIGURING THE MATCH LEVEL

*The match level* is the number of table data cells against which the application is searching SharePoint for matches. The number of cells involved in the search is defined as the number of unique intersections between columns and lines in the table. The match level has two parameters:

- **Threshold value of rows**. The minimum number of rows containing data for which the application searches SharePoint for matches.
- **Threshold value of columns**. The minimum number of columns containing data for which the application searches SharePoint for matches.

By finding a match to table data, the application detects a file containing data from the specified number of columns in the specified number of rows. There is no requirement for the same columns to match in different rows.

**Example:**

A table of CSV format containing the following table data has been added to the category:

| Column 1 | Column 2 | Column 3 | Column 4 | Column 5 |
|---|---|---|---|---|
| 1946 | 2718 | 0 | 0 | 0 |
| 3376 | 2753 | 58 | 1 | 4 |
| 3370 | 2746 | 67 | 9 | 4 |
| 3373 | 2731 | 6 | 1 | 7 |

The following match level for table data is configured: the threshold value of rows is 2, the threshold value of columns is 3.

The application detects files whose data match six cells of table data. The matching data must be located in at least two rows at once, and at least three cells must produce a match in each row. For example:

| Column 1 | Column 2 | Column 3 | Column 4 | Column 5 |
|---|---|---|---|---|
| 1946 | 2718 | 0 | 0 | 0 |
| 3376 | 2753 | 58 | 1 | 4 |
| 3370 | 2746 | 67 | 9 | 4 |
| 3373 | 2731 | 6 | 1 | 7 |

Given this match level, the application will also detect a file containing the following table data:

| Column 1 | Column 2 | Column 3 | Column 4 | Column 5 |
|---|---|---|---|---|
| 1946 | 2718 | 0 | 0 | 0 |
| 3376 | 2753 | 58 | 1 | 4 |
| 3370 | 2746 | 67 | 9 | 4 |
| 3373 | 2731 | 6 | 1 | 7 |

Files with a lesser number of matches are ignored by the application. For example:

| Column 1 | Column 2 | Column 3 | Column 4 | Column 5 |
|---|---|---|---|---|
| 1946 | 2718 | 0 | 0 | 0 |
| 3376 | 2753 | 58 | 1 | 4 |
| 3370 | 2746 | 67 | 9 | 4 |
| 3373 | 2731 | 6 | 1 | 7 |

In the example above, table data in three cells match a CSV table only in one row. The file does not match the specified threshold value of rows (2) and is therefore ignored by the application.

# REFRESHING THE LIST OF INCIDENTS

The list of incidents is not refreshed automatically. To manage new incidents, the list of incidents has to be refreshed manually.

*To refresh the list of incidents:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Incidents** node.
3. Click the **Refresh** button in the workspace of the node.

New incidents created since the time when the list was refreshed last are added to the list.

# SEARCHING FOR INCIDENTS USING A FILTER

By default, the list of incidents displays all incidents irrespective of their generation time and current status. You can filter the list of incidents to display only incidents with a particular status or incidents generated during a certain period.

*To find an incident using a filter:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Incidents** node.
3. Configure the incident filtering condition in the **Incident filter** section.

   Each filtering condition has two parameters: a criterion and a value. The drop-down list on the left lets you select an incident filtering criterion. Incident details are used as filtering criteria. In the drop-down list next to it you can specify the value of the selected criterion according to which filtering is performed. The appearance of the drop-down list depends on the filtering criterion selected.
4. If necessary, specify additional conditions by clicking the **Add a condition** button.

   The application performs filtering according to all conditions added to the incident filter.
5. Click the **Search** button to search for incidents.

The **List of incidents** section displays incidents that meet the search conditions.

# SEARCHING FOR POLICIES SPECIFIC TO USERS

*To search for policies created for specific users:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Categories and policies** node.
3. In the **Policy search** section, choose one of the following search options:

   - **On users without Active Directory accounts** – to find policies configured for anonymous users and users without Active Directory accounts.
   - **On selected users** – to find all policies configured for specific users who have Active Directory accounts.

     Click the **Select** button to specify a user account for running a policy search. You cannot select multiple user accounts.
4. Click the **Find** button start the policy search.

The application displays the list of policies located. For each policy, the application displays the corresponding data category and the action taken by the application when this policy is violated. If the policy that has been found is inactive, the relevant information is displayed in the **Action** column.

# SEARCHING FOR SIMILAR INCIDENTS

*To find similar incidents:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Incidents** node.
3. In the list of incidents, select an incident whose details you want to view.
4. Right-click to open the context menu of the incident and select **Find similar incidents**.

   This opens a list of criteria for finding incidents that are similar to the selected one.
5. Select a criterion to find similar incidents:
   - **Same category**.
   - **Same policy**.
   - **Same file**.
   - **Same user**.

The application automatically defines the incident filtering conditions in accordance with the selected criterion. The **List of incidents** section displays incidents that meet the search conditions.

# VIEWING INCIDENT DETAILS

*To view incident details:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the Incidents node.
3. In the list of incidents, select an incident whose details you want to view.
4. Click the **View** button.

   The **Incident details** window opens. In this window, you can view detailed information about the incident, change its status, and select an action for the incident-related file. You can switch between incidents in the list by clicking the **Previous** and **Next** buttons.

   The **View** tab shows the details of incidents and the reasons why they were generated.

   The **History** tab shows information about the history of incident processing (such as changes of the incident status or incident archiving).
5. Click the **Cancel** button to finish viewing the incident details.

If you changed the incident status while viewing the incident details, click **OK** to save changes.

# VIEWING THE REPORT ON POLICY-RELATED INCIDENTS

*To view the report on policy-related incidents:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Reports** node.
3. In the list of reports, open the **View and create reports** section and select the report for which the **Policy-related incidents type** is displayed in the **Report type** column.
4. Click the **View** button.

The report opens in the default browser.

The report contains the following information:

- Report parameters:
  - Report type.
  - Date and time of report generation.
  - Number of incidents selected for the report.
  - The reporting period.
  - The statuses based on which the application has selected incidents for the report.
  - The users for which the application has selected incidents for the report.
  - The categories and policies based on which the application has selected incidents for the report.
- List of incidents selected for the report.

  The list of incidents contains a table with detailed information on each incident included in the report. Incidents in the table are arranged in the order of the incident details selected in the report settings.

# VIEWING THE SYSTEM KPI REPORT

*To view the system KPI report:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the Reports node.
3. In the list of reports, open the View and create reports section and select the report for which the System KPI type is displayed in the Report type column.
4. Click the View button.

The report opens in the default browser.

The report contains the following information:

- Report parameters:
  - Report type.
  - Date and time of report generation.
  - The reporting period.

- KPI data:
  - **In scope of policies**. Number of files whose data has been scanned by the application.
  - **Clean**. Number of files that have not been found to contain any data matching the categories.
  - **Violations**. Number of files that have been found to contain data matching the categories.
  - **Errors**. Number of files whose data has not been scanned due to errors (such as errors caused by the absence of access to user details).
  - **Scan timeouts**. Number of files whose data has not been scanned due to scan timeouts.
  - **Beyond scope of policies**. Number of files whose data has not been scanned because the users or SharePoint sites related to them are not specified in the policy settings.
  - **Total**. Number of files processed by the application during the specified period.
- Violation data:
  - List of categories whose policies were violated during the reporting period. The number and ratio of category-specific violations to the total number of violations (in percentage points) is displayed for each category.
  - **Total**. Number of violations across all categories.

# VIEWING THE REPORT ON USERS

*To view the report on users:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Reports** node.
3. In the list of reports, open the **View and create reports** section and select the report for which the **User statistics type** is displayed in the **Report type** column.
4. Click the **View** button.

The report opens in the default browser.

The report contains the following information:

- Report parameters:
  - Report type.
  - Date and time of report generation.
  - Number of incidents selected for the report.
  - The reporting period.
  - The statuses based on which the application has selected incidents for the report.
  - The users for which the application has selected incidents for the report.
  - The categories and policies based on which the application has selected incidents for the report.
- The incident table.

  The **Number of incidents by categories on users' side** table contains a list of incidents selected for the report. For each user, the application displays the name of the department where the user works, the number of incidents associated with the user, and the names of categories to which these incidents belong.

# VIEWING THE INCIDENT STATUS REPORT

*To view the incident status report:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Reports** node.
3. In the list of reports, open the **View and create reports** section and select the report for which the **Incident status statistics type** is displayed in the **Report type** column.
4. Click the **View** button.

The report opens in the default browser.

The report contains the following information:

- Report parameters:
  - Report type.
  - Date and time of report generation.
  - Number of incidents selected for the report.
  - The reporting period.
  - The categories based on which the application has selected incidents for the report.
- The incident table.

  The **Number of incidents by policies** table contains a list of incidents selected for the report. Each category is shown with the policies configured for this category. The number of incidents created during policy violations is specified for each policy, along with the current status of all incidents.

# VIEWING THE SEARCH RESULTS

*To view the search results:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Search** node.
3. In the list of reports in the **Search results** section, select a report and click the **View** button.

The report opens in the default text editor.

The report contains the following information about the search results:

- Task settings:
  - SharePoint sites on which the search was performed;

    If the SharePoint sites specified in the search settings cannot be accessed, the report shows only their addresses and access error information.
  - Categories according to which the search was performed.
  - Reasons why the task ended (for example, the task was stopped manually).
- Search start and end times.

- Number of files scanned.
- List of files matching the search settings. The following information is displayed for each file:
  - File name and format;
  - Full path to the file on the SharePoint site;
  - File version;
  - Name of the user that uploaded the file to the SharePoint site (first version of the file);
  - Name of the user that made the last changes to the file (last file version);
  - Date and time when file scanning started;
  - Name of the category of data detected in the file.

    If data belonging to several categories has been detected in the file, information about each category detected is displayed in a separate table column.

    If the file has been found to contain data of the table data category, the report shows the number of rows from the CSV file loaded into the category.
- Possible error information:
  - Access to the file is blocked
  - The file could not be opened
  - The file could not be scanned

# VIEWING PROTECTION STATUS DETAILS

Information about the status of data protection is displayed in the workspace of the **Data Leak Prevention** node of Administration Console.

The **DLP Module status** section displays information about the current status of the Module and any notifications about Module errors:

- *Enabled*. The administrator of Kaspersky Security has enabled the DLP Module, and the application runs correctly on all servers.
- *Enabled, running with errors*. The administrator of Kaspersky Security has enabled the DLP Module, but the application has encountered errors during its operation. The application shows error information in the lower part of the section. For each type of error, the application shows the names of servers where errors of this type were detected. The following types of errors are possible:
  - *Scan errors.* The application is unable to scan files due to time-out, infrastructure errors, or interceptor errors.
  - *DLP Module license error*. The application is unable to scan files because a DLP Module license is missing, the license has expired, or the key has been black-listed.
  - *Server unavailable*. The application is unable to scan files because there is no access to the SharePoint server (the server may have been disabled by the administrator).
- *Disabled*. Administrator disabled the DLP Module. The application does not scan files uploaded by users to SharePoint.

The **Opened incidents** section displays the following information about users and currently opened incidents:

- The number of unique users with whom opened incidents are associated
- The rating of users with the highest number of policy violations
- The number of incidents with *New* status
- The number of incidents with *In progress* status.

Data on the ratio of incidents with *New* status to incidents with *In progress* status is presented in the form of a chart. The chart shows statistics on incidents associated with the selected categories of data. You can modify the list of categories for which statistics are displayed (see section "Selecting categories for generating incident statistics" on page 25).

The **Statistics** section lets you view information on files scanned and incidents closed over periods of 7 days or 30 days. Depending on the period selected, the following indicators change:

- The number of files uploaded by users to SharePoint
- The number of files scanned by the application
- The number of incidents generated
- The number of files that have not been scanned due to time-out
- The number of files that have not been scanned due to errors

Information on the reasons why incidents have been closed is presented in the form of a chart. The chart shows statistics on incidents associated with the selected categories of data. You can modify the list of categories for which statistics are displayed (see section "Selecting categories for generating incident statistics" on page 25).

# GENERATING A QUICK REPORT

*To create a quick report, perform the following steps:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Reports** node.
3. In the **View and create reports** section, click the **New report** button.
4. Select the type of report you are creating in the drop-down list.
5. In the window that opens, configure the report generation settings.
6. Click **OK** to begin generating the report.

The final report is displayed in the list of reports in the **View and create reports** section and automatically opens in the browser window.

# SAVING REPORTS

*To save a report:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Reports** node.

3. In the list of reports in the **View and create reports** section, select a report to be saved and click the **Save** button.
4. In the window that opens, specify the folder to save the report to and click the **Save** button.

The application saves the report in an HTML file to the specified folder. By default, the name of the file being saved matches the report name.

# SAVING SEARCH RESULTS

*To save search results:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Search** node.
3. In the list of reports in the **Search results** section, select a report and click the **Save** button.

The application saves the report in CSV format to the specified folder.

# DELETING ARCHIVED INCIDENTS

*To delete archived incidents:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Incidents** node.
3. Click the **Delete archived** button under the list of incidents.

After deletion is confirmed, the application removes incidents with *Archived* status from the incident list.

# DELETING A TASK

*To delete a search task:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Search** node.
3. In the list of tasks in the **Search tasks** section, select a task to delete and click the **Delete** button.

After you confirm deletion, the application deletes the task permanently.

# DELETING A CATEGORY

*To delete a category:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Categories and policies** node.
3. In the list of categories, select the category to be deleted and click the **Delete** button.

After you confirm deletion, the application deletes the category permanently.

If polices were assigned to this category, they are deleted together with the category.

If the deleted category was used in search tasks, the task settings are modified after the category has been deleted.

# DELETING A REPORT

*To delete a report:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Reports** node.
3. In the list of reports in the **View and create reports** section, select a report to be deleted and click the **Delete** button.

   You can delete several reports at once.

After you confirm deletion, the application deletes the selected reports permanently.

# DELETING A POLICY

*To delete a policy:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Categories and policies** node.
3. Select the category of confidential data for which you want to delete the policy and click the button  .

   This opens a list of policies assigned for the category.
4. Select the policy you want to delete in the list and click the Delete button.
5. Confirm deletion of the policy in the dialog box.

The application deletes the policy permanently.

# DELETING THE SEARCH RESULTS

*To delete search results:*

1. Open Administration Console.
2. In the Administration Console tree of nodes, select the **Search** node.
3. In the list of reports in the **Search results** section, select reports to delete and click the **Delete** button.

After you confirm deletion, the application deletes the selected reports on search results permanently.

# GLOSSARY

## A

### Active policy

The policy that the application is currently using for monitoring data leakage. The application can use multiple policies concurrently.

### Archived incident

An incident that was restored from an archive to Administration Console for further use (e.g., for finding information about similar violations of a policy that were recorded earlier).

### Archiving

A process of moving closed incidents to an archive in protected format. After archiving incidents, the application deletes them from Administration Console.

## C

### Closed incident

An incident that was processed completely, with a decision made regarding this incident.

### Confidential data

Information that is not subject to disclosure and distribution beyond a limited circle of people. Confidential data usually include information that encloses a state or commercial secret, as well as personal data.

### Control scope

SharePoint websites for which the application monitors file uploading. When the user uploads a file to a website within the control scope, the application scans the file for data protected by the active policies.

### Corporate security

A scope of regulations and measures aimed at the protection of a company's business interests. This may be, e.g., collection of information about the company's internal environment or its competitors, analysis of market trends, and protection of intellectual property.

## D

### DLP Module (Data Leak Prevention)

Component of Kaspersky Security that is designed for the protection of data published on SharePoint websites against leakage.

### DLP Module status

The current state of DLP Module. With the DLP Module status, Kaspersky Security informs of errors in the operation of DLP Module and ways of eliminating them.

### Data category

A set of data sharing a common feature or subject and meeting specific criteria (e.g., a set of words that come in a text in a specified order). The application uses data categories for recognizing information in files being uploaded and stored on SharePoint. The application allows using preset Kaspersky Lab data categories and creating custom data categories.

### DATA LEAK PREVENTION

The scope of a security officer's actions aimed at preventing any unauthorized access to confidential information (such as blocking a file when it is uploaded to SharePoint).

### DATA LEAKAGE

Unauthorized access to confidential data and further uncontrolled distribution.

### DATA SEARCH

Search for data from specified categories on SharePoint websites. The application searches for data in accordance with the settings of the search task.

### DATA SUBCATEGORY

A nested data category included in a larger-scale category. Each subcategory describes a set of category data combined with a common feature. For example, the "Magnetic stripe data" subcategory belongs to the "Payment cards" category. You can change the contents of a category by including or excluding subcategories. For example, you can exclude the subcategories that the application must not use to monitor data leakage.

## F

### FALSE POSITIVE INCIDENT

An incident that shows apparent signs of a data leak when no leakage is detected. For example, a false positive incident may be registered when the user attempts to upload a file that contains no financial information but is used as a template for financial accounting.

### FILE BLOCKING

The application's action aimed at a possible data leak. The application can block a file that initiated a policy violation. If the application blocks a file, the user cannot upload the file to SharePoint.

### FULL SCAN

A type of file scan. When performing a full scan, the application searches for data from the specified categories in all files stored on SharePoint servers.

## I

### INCIDENT

A record of an application event associated with a possible data leak. The application creates an incident, e.g., when a policy is violated.

### INCIDENT DETAILS

Detailed information about the incident.

### INCIDENT STATUS

The current state of an incident. The status indicates the incident processing stage. The statuses of incidents can be used for managing the process of handling incidents.

### INCREMENTAL SCANNING

A type of scheduled file scan. During an incremental scan, the application searches for data on SharePoint servers, only scanning files that have been modified since the previous scan.

## K

### KPI (KEY PERFORMANCE INDICATORS) OF THE SYSTEM

Application report type Contains detailed information about the key performance indicators of DLP Module.

### KASPERSKY LAB CATEGORIES

Predefined data categories developed by Kaspersky Lab specialists. Those categories can be used for monitoring data leaks and data search through files that are uploaded and stored on SharePoint. Categories can be updated when updating the application databases. A security officer cannot modify or delete predefined categories.

### KEYWORDS

Word, phrase, or sequence of characters that the application uses for recognizing data in files being uploaded and stored on SharePoint. Keywords can be added to a data category.

## M

### MATCH LEVEL

Criterion showing how well the information in files being uploaded and stored on SharePoint matches a table data category. The match level can be set up when creating or modifying a table data category.

A security officer can specify the number of cells that will impact the match level. The number of cells is defined as the number of unique intersections between columns and rows in the table.

## O

### OPENED INCIDENT

An incident that has been assigned the New or In processing status.

## P

### PERSONAL DATA

Information that allows identifying a person, directly or indirectly.

### POLICY

A named collection of application settings used for the protection of data against leakage. A policy includes configured conditions for uploads of confidential information to SharePoint servers, as well as the application's actions on detection of a possible data leak.

### POLICY VIOLATION

The user's actions leading to a violation of the conditions applied to the upload of confidential information on SharePoint servers. The user violates a policy when uploading to SharePoint (or sending by email) some data from a policy-protected category.

## S

### SEARCH SCOPE

SharePoint websites on which the application searches for data. If files are stored on a website within the search scope, the application scans the files for data from the categories specified in the search task.

### SEARCH TASK

A set of criteria and parameters based on which the application searches for data on SharePoint servers.

### SECURITY OFFICER

An employee who is in charge of controlling compliance with the corporate security requirements on SharePoint servers, as well as monitoring and preventing data leakage.

## T

### TABLE DATA

Information organized in table format. When handling table data in Kaspersky Security, CSV (Comma Separated Values) files must be used.

## U

### USER CATEGORY

A data category that has been created by a security officer.

## V

### VIOLATION CONTEXT

A text fragment with data that violates a policy when uploaded to SharePoint servers. The violation context is required when making a decision on an incident.

## W

### WORKING SCENARIO

A sequence of actions that is recommended to a security officer for solving a standard task. A scenario includes both actions in the application interface and preparatory actions beyond the application (such as planning or analysis).

# 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.

Active Directory, Excel, SharePoint, SQL Server, Windows are trademarks of Microsoft Corporation registered in the United States of America and elsewhere.

# INDEX

## M



## N



## P



## R



## T