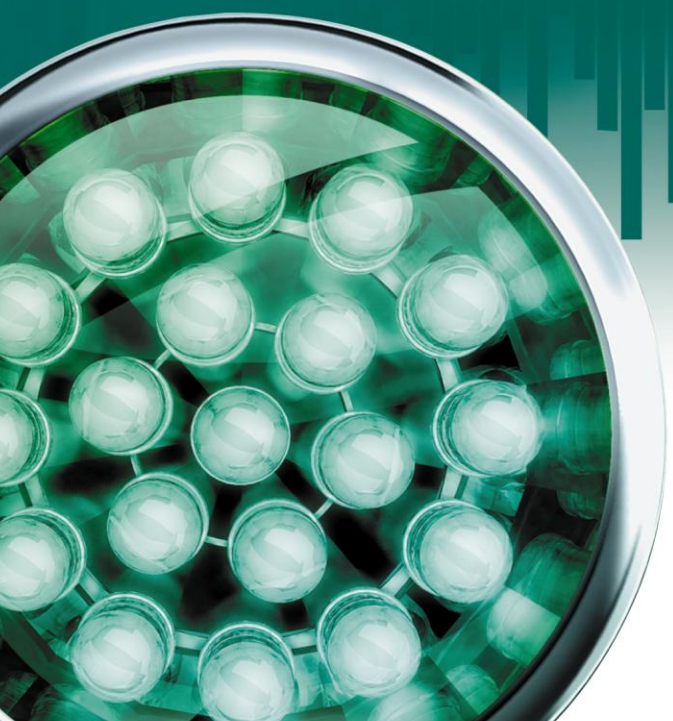
Kaspersky Administration Kit 8.0

GETTING STARTED

PROGRAM VERSION: 8.0 CRITICAL FIX 1



KASPERSKY lab

Dear User!

Thank you for choosing our product. We hope that this documentation 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 at the Kaspersky Lab website, at http://www.kaspersky.com/docs.

Revision date: 2/2/10

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

CONTENTS

INTRODUCTION

This document describes the basic steps which an anti-virus security administrator should take to start using **Kaspersky Administration Kit**, and to deploy Kaspersky Lab's anti-virus applications across the managed network.

This document describes in detail a simple installation scenario, in which an anti-virus application is only deployed on several computers running the Microsoft Windows operating system without the use of a hierarchy of administration servers.

This is a typical scenario for deployment across networks in small or medium-size companies, to which the following conditions apply:

- Computers run operating systems which satisfy system requirements (for details, please consult the Deployment Guide).
- Some of the computers belong to a domain and some belong to groups.
- The network includes a domain controller.
- The name service is based on the NetBIOS protocol.

This document also describes how to upgrade from version 6.x to version 8.0.

Detailed information about the Kaspersky Administration Kit is contained in the Deployment Guide, the Administrator's Guide and the Reference Guide.

Kaspersky Administration Kit enables Kaspersky Lab's anti-virus applications to be administered as a single system, across a network. Using the Administration Kit, an administrator can:

- Create administration groups to ensure anti-virus protection for the company, which allow similar types of computers to be managed as a single unit.
- Remotely install and uninstall Kaspersky Lab's anti-virus applications.
- Centrally administer all installed anti-virus applications across the network, from a single computer.
- Centrally receive and distribute on network computers database updates and application modules of anti-virus programs.
- Receive notifications about critical events in the operation of the anti-virus applications.
- Receive statistics and reports about the operation of the anti-virus applications.
- Manage licenses for all installed anti-virus applications.
- Centrally manage objects put in Quarantine or Backup by anti-virus applications, and also objects for which disinfection has been postponed.
- Centrally manage any third-party applications installed within the network.

Kaspersky Administration Kit consists of three major components:

- **Administration Server** centralizes the storage of information about Kaspersky Lab's applications installed in the corporate network and about their management.
- **Network Agent** coordinates the interaction between Administration Server and installed Kaspersky Lab applications on a particular network node (workstation or server). This component supports all the Windows

applications in Kaspersky's Open Space Security range. Separate versions of Network Agent exist for Kaspersky Lab's Novell and Unix applications.

- **Administration Console** provides a user interface to the administration services of the Administration Server and Network Agent. The management module is implemented as a snap-in for the Microsoft Management Console (MMC).

OBTAINING INFORMATION ABOUT THE APPLICATION

If you have any questions regarding purchasing, installing or using Kaspersky Administration Kit, answers are readily available.

Kaspersky Lab provides various sources of information about the application. You can choose the most suitable, according to the importance and urgency of your question.

IN THIS SECTION

INFORMATION SOURCES FOR FURTHER RESEARCH

You can view the following sources of information about the application:

- the application's page on Kaspersky Lab's website;
- the application's Knowledge Base page on the Technical Support Service website;
- electronic help system;
- documentation.

The application's page at the Kaspersky Lab website

http://www.kaspersky.com/administration_kit

This page will provide you with general information about the application's features and options.

The application's Knowledge Base page at the Technical Support Service website

http://support.kaspersky.com/remote_adm

This page contains articles by the Technical Support Service.

These articles contain useful information, recommendations, and the Frequently Asked Questions (FAQ) page, and cover purchasing, installing and using the application. The articles are sorted by subject, such as "License management", "Database updates", and "Troubleshooting". The articles aim to answer questions about not only this application but other Kaspersky Lab products as well. They may also contain news from the Technical Support Service.

The electronic help system

The application installation package includes full help files, which contain step by step descriptions of the application's features.

To open the help file, select **Kaspersky Administration Kit help system** in the console **Help** menu.

If you have a question about a specific application window, you can use context-sensitive help.

To open context-sensitive help, in the corresponding window, press the **Help** button or the **F1** key.

Documentation

The documentation supplied with the application aims to provide all the information you will require. It includes the following documents:

- **Administrator's Guide** describes the purpose, basic concepts, features and general schemes for using Kaspersky Administration Kit.
- **Deployment Guide** contains a description of the installation procedures for the components of Kaspersky Administration Kit as well as remote installation of applications in computer networks using simple configuration.
- **Getting Started** guide gives a step by step guide to anti-virus security administrators, enabling them to start using Kaspersky Administration Kit quickly, and to deploy Kaspersky Lab's anti-virus applications across a managed network.
- **Reference Guide** contains an overview of Kaspersky Administration Kit, and step by step descriptions of its features.

The documents are supplied in PDF format in Kaspersky Administration Kit's distribution package (installation CD).

You can download the documentation files from the application's page at Kaspersky Lab's website.

CONTACTING THE TECHNICAL SUPPORT SERVICE

You can obtain information about the application from the Technical Support Service, by phone or on the Internet. When contacting the Technical Support Service, you will need to provide information about the license for the Kaspersky Lab product with which you are using the application.

The Technical Support Service will answer any questions related to the installation and use of the application that are not covered in help topics. If your computer has been infected, they will help you to neutralize the consequences of malware activity.

Before contacting the Technical Support Service, please read the support rules for Kaspersky Lab's products http://support.kaspersky.com/support/rules.

Technical Support by email

You can send your question to the Technical Support Service by filling out a Helpdesk web form for client questions at http://support.kaspersky.com/helpdesk.html.

You can ask your question in Russian, English, German, French or Spanish.

To send an email request, you should specify your **customer ID**, which you received while registering at the Technical Support Service's website, and the corresponding **password**.

If you are not yet a registered user of Kaspersky Lab's applications, you can fill out a registration form (https://support.kaspersky.com/en/personalcabinet/registration/form/). During registration you will need to enter either your application's *activation code*, or indicate the *key file*.

The Technical Support service will respond to your request in your Personal Cabinet https://support.kaspersky.com/en/PersonalCabinet), and to the email address you specified in your request.

In the website's request form, please describe the problem you have encountered. In the mandatory fields, specify:

- **Request type**. Questions which users often ask divided into separate topics, for example: "Problems with Setup / Remove application" or "Virus disinfection". If you do not find an appropriate topic, select "General question".
- **Application name and version number**.
- **Request description**. Describe the problem you encountered in as much detail as possible.
- **Customer ID and password**. Enter the client number and the password you received when you registered at the Technical Support Service's website.
- **Email address**. The Technical Support Service will reply to your question at this email address.

Technical support by phone

If you have an urgent problem, you can call your local Technical Support Service. Before contacting Russian-speaking (http://support.kaspersky.ru/support/support_local) or international (http://support.kaspersky.com/support/international) Technical Support, please have the necessary information (listed at http://support.kaspersky.com/support/details) about your computer to hand. This will let our specialists help you more quickly.

DISCUSSING KASPERSKY LAB'S APPLICATIONS ON THE WEB FORUM

If your question does not require an immediate answer, you can discuss it with Kaspersky Lab's experts and other users in our forum at http://forum.kaspersky.com.

In this forum you can view existing topics, leave your comments, create new topics and use the search engine.

GETTING STARTED

To ensure comprehensive anti-virus protection of your company:

- Deploy anti-virus protection on the computers within the network (see section "Deployment of Anti-Virus Protection" on page 8).
- Perform daily tasks (on page 14), which would allow to trace the current status of anti-virus protection.
- Periodically perform additional tasks (see section "Periodic tasks" on page 16), to keep the anti-virus up-to-date state and respond to any problems arising in timely fashion.

The following sections of this document give more detailed descriptions of these actions.

IN THIS SECTION

DEPLOYING ANTI-VIRUS PROTECTION

To deploy anti-virus protection across the corporate network:

1. Install the Administration Server and the Administration Console (see section "Installing Kaspersky Administration Kit" on page 9).
2. Modify the initial settings, and deploy the corporate anti-virus protection system using the Quick Start Wizard (see section "Initial anti-virus protection configuration" on page 9).
3. Create administration groups (see section "Creating an administration group" on page 11) and add client computers to them. Administration groups can manage a collection of client computers as a single unit, using policies and group tasks.
4. Remotely install, on selected client computers, Kaspersky Lab anti-virus applications which support management through Kaspersky Administration Kit (see section "Remote installation of anti-virus applications" on page 11). At this stage you should also verify that the installed anti-virus applications are operating correctly on the client computers.
5. Verify that the application databases are being correctly updated on the client computers (see section "Verifying database updates" on page 12).
6. Configure settings of notification about events in the operation of the anti-virus protection on client computers (see section "Configuring notifications" on page 12).
7. Run on-demand scan task and verify the operation of notifications about events in the anti-virus security system operation on client computers (see section "Verification of the distribution of notifications and on-demand scan task" on page 13).
8. View reports and configure automatic delivery of the required reports by email (see section "Receiving reports" on page 13).
9. Configure the automatic installation of anti-virus applications on new networked computers (see section "Configuring the automatic installation of applications" on page 14).

When these actions have been completed, the anti-virus protection system will be deployed across the company's network.

INSTALLING KASPERSKY ADMINISTRATION KIT

To install the Administration Server and the Administration Console:

1. Select the computer on which the components will be installed. You are advised to install the Administration Kit on a computer which is a member of the domain.

   You can install the Administration Server and the Kaspersky Administration Kit Console 8.0 on the same computer where the Administration Server and the Console versions 5.x and 6.x are running.

   You are advised to perform the installation using domain administrator's rights. This will allow the automatic creation of the **KLAdmins** and **KLOperators** groups, and provide the necessary rights to the account under which Administration Server will be running.

2. Run the executable file setup.exe from the installation CD, and follow the installation wizard's instructions.

3. Select standard installation. Most of the settings will be determined automatically.

   Custom installation is described in detail in the Kaspersky Administration Kit Deployment Guide.

   Programs required for the application's operation, will be installed on the computer if they have not been already installed:

   - Microsoft Windows Installer 3.1;
   - Microsoft Data Access Components (MDAC) 2.8;
   - Microsoft .NET Framework 2.0;
   - Microsoft SQL Server 2005 Express Edition.

   These ancillary applications do not require any maintenance or administration.

During the wizard's next stage, the application's files will be copied to the computer, and the database will be created in which Administration Server stores information about the company's anti-virus protection.

After the wizard is completed, you can start the Administration Console and perform initial configuration of the application settings (see section "Initial anti-virus protection configuration" on page 9).

You can also choose to install the Administration Console on a separate computer, and manage the Administration Server across the network. To do this, specify Custom installation in the setup wizard, and in the component selection window, check only the box beside the **Administration Console** component.

After installing the Administration Console, you must connect to the Administration Server to be managed, by starting the Administration Console. In the window that opens, specify the name of the computer on which Administration Server is installed, and the settings of the account used to connect to it. After the connection has been established, you can manage the anti-virus protection system fully.

INITIAL ANTI-VIRUS PROTECTION CONFIGURATION

Initial anti-virus protection is configured by the wizard, which opens when Administration Console runs for the first time.

To perform an initial configuration of the company's anti-virus protection using the Quick Start Wizard:

1. Specify the license which will be used by the applications managed through Kaspersky Administration Kit, and specify whether it should be automatically applied to new computers as they are added to administration groups. You can choose to skip this action, and add a license later.

2. Wait until the Administration Server finishes polling the network and detects all networked computers.

3. Configure the email notification system, which will provide information about the operation of the anti-virus protection. You can modify these settings later in the Administration Server's properties (for more details please refer to the Reference Guide).

4. Start creating policies and tasks for anti-virus applications, which are used to ensure that the anti-virus protection systems function correctly across the corporate network. Policies in Kaspersky Administration Kit define general settings for the administered applications' operation, and tasks define how the applications will perform specific actions.

   The following objects will be created:

   - Upper level policies for Kaspersky Anti-Virus for Windows Workstations and Kaspersky Anti-Virus for Windows Servers, with default settings. You can view and modify policy settings later. To prevent users from changing a policy's settings, use the  sign for these settings.

   - Upper level group tasks to update the application databases on client computers, using default settings (for Kaspersky Anti-Virus for Windows Workstations and for Kaspersky Anti-Virus for Windows Servers). These tasks are configured so that the client computers receive updates from the Administration Server.

     For detailed information about other ways to obtain updates, visit Kaspersky Lab's website (http://www.kaspersky.com/avupdates).

   - Virus scan tasks for client computers using default settings (for Kaspersky Anti-Virus for Windows Workstations and Kaspersky Anti-Virus for Windows Servers).

   - An Administration Server task which downloads updates from the Internet, with default settings.

     This task receives updates for the application databases and application modules from Kaspersky Lab's update servers, and puts them in the shared folder specified during the installation of Administration Server. Client computers can copy their updates from this shared folder on the Administration Server using data stored in the shared folder. Later you can fine-tune the update process for client computers, by distributing updates to slave Administration Servers, and using Update Agents.

   - An Administration Server backup task with default settings. This task creates a backup copy of the Administration Server's data, including its information database, the structure of administration groups, the available installation packages, and the Administration Server's certificate.

   - An Administration Server task for delivering reports. By default, Administration Server sends a daily report about the level of anti-virus security to the email address specified in the Quick Start Wizard.

   After creating these policies and tasks, Administration Server will launch the updates task. You can move on to the next step of the wizard without waiting for this task to complete.

   Information about updates placed into the shared folder will be displayed in the console tree in the **Repositories** → **Updates** folder.

5. In the final window specify whether you wish to launch the Deployment wizard immediately after the Quick Setup Wizard completes (see section "Remote anti-virus application installation" on page 11).

CREATING AN ADMINISTRATION GROUP

To add a new administration group:

1. In the console tree select the group which should include the new group.
2. In the task pane, select the **Groups** tab, and click the **Create a subgroup** link.
3. In the window that opens, enter the name for the new group and click **OK**.

   After that, the Administration Console will open on the folder of the created group.
4. Move the required client computers from the **Unassigned computers** folder to the administration group created. To do this, use the **Add computers to the group** link on the task pane, and follow the wizard's instructions.

The added computers will be shown for the group in the results pane in the **Client computers** nested folder.

To create a set of computers to be moved to the administration group, according to any set criteria, open the context menu of the **Unassigned computers** folder and select the **Search** item. When the required computers have been found, use the **Move to Group** context menu command. For details, please see the Kaspersky Administration Kit Administrator's Guide.

REMOTE INSTALLATION OF ANTI-VIRUS APPLICATIONS

This section describes the remote installation of Kaspersky Anti-Virus for Windows Workstations. The remote installation procedure is similar for all of Kaspersky Lab's other anti-virus applications.

Some Kaspersky Lab's applications can be managed via Kaspersky Administration Kit, but can only be locally installed on client computers (for details, please refer to the Guides for the corresponding applications).

To remotely install Kaspersky Anti-Virus for Windows Workstations:

1. In the console tree, select the Administration Server node.
2. In the **Deployment** section of the task pane, click the **Install Kaspersky Anti-Virus** link to go to the anti-virus setup wizard.
3. In the wizard that opens, select the Kaspersky Anti-Virus for Windows Workstations installation package. This package is created during the installation of the Administration Server, and contains the application's default settings. Network Agent is always installed with the application.
4. Specify either the computers, or the administration group, which are the target hosts for the application installation.
5. Specify the license key file, if it was not specified when creating the installation package.
6. Specify whether the host computers should be restarted after installing Kaspersky Anti-Virus for Windows Workstations.
7. If a collection of hosts was selected earlier for the installation, specify whether you wish to move them to another administration group.
8. Specify an account to be used to access client computers. If the Administration Server's account has administrator's rights on client computers, select the **Install through Network Agent** option.
9. Start remotely installing the application.

When the remote installation task is completed, Kaspersky Anti-Virus for Windows Workstations and Network Agent will both be installed on the specified host computers.

Remote installation can be performed on computers with Kaspersky Anti-Virus for Windows Workstations 5.x or 6.x installed. In this case, Kaspersky Anti-Virus 5.x or 6.x will be removed and Kaspersky Anti-Virus 6.0 MP4 will be installed instead.

To check that the installation was successful, either select the **Client computers** folder of the corresponding administration group or locate the required computers in the results pane, in the **Unassigned computers** folder and view information in the **Agent/Anti-virus** column. If the column contains two plus (+) signs, both Network Agent and Kaspersky Anti-Virus for Windows Workstations were successfully installed. The **Real-time protection status** column must contain the value **In progress**.

VERIFYING DATABASE UPDATES

The anti-virus protection system can operate correctly only if the latest database versions are available. Therefore, it is necessary to check that the task of downloading updates to the repository (shared folder) on the Administration Server, and the task of distributing those updates to the client computers, are both operating correctly.

To check database updates:

1. In the Administration console navigate to the **Kaspersky Administration Kit tasks** folder and select the task of downloading updates to the repository.
2. Open the task properties window, by selecting **Properties** in the context menu.
3. Select the **Updates testing** tab.
4. Check the **Test updates before distributing** box.
5. In the **Updates testing task** field, select a task from the existing tasks with the **Select** button. You can also create a new updates testing task. To do this, click the **Create new task** button and follow the wizard's instructions. During creation of a new updates testing task, the Administration Server generates test policies, and auxiliary group update and on-demand scan tasks.

   It is recommended to run the updates testing task on well-protected computers with the software configuration most typical of your corporate LAN. This approach increases the quality of scans, and minimizes the risk of false responses and the probability of virus detection during scans. If viruses are detected on the test computers, the update testing task will be considered failed.

After the specified settings are applied, the updates testing task will be started before distribution of databases. The Administration Server will download updates from the source, save them to a temporary storage, and run the updates testing task. If the task completes successfully, the updates will be copied from the temporary storage to the shared folder on the Administration Server and distributed to all other computers for which the Administration Server is the source of updates.

If the results of the updates testing task show that updates located in the temporary storage are incorrect or if the updates testing task completes with an error, such updates will not be copied to the shared folder, and the Administration Server will keep the previous set of updates. The tasks using the **When new updates are downloaded to the repository** schedule type are not started then, either. These operations will be performed at the next start of the Administration Server updates download task if testing of the new updates completes successfully.

CONFIGURING NOTIFICATIONS

To configure notifications about events in the operation of the anti-virus system:

1. Select a policy for the anti-virus application in the **Policies** folder in the administration group (for example, Kaspersky Anti-Virus for Windows Workstations).
2. In the task pane in the **Actions** section, click the **Configure notifications** link to go to the configuration of notifications about events.

3. Select the required events and specify notification delivery methods for them. To do this, click the **Properties** button and check the boxes beside the required notification methods, in the **Event notification** section:

   - Notify by email.
   - Notify through NET SEND.
   - Notify by running executable file;
   - Notify via SNMP.

   To verify the distribution of notifications, it is sufficient to set notification for the **Detection of Viruses, Worms, Trojans, and Malware** and **Detection of possibly infected object** events (see section "Verifying the notification system and on-demand scan tasks" on page 13).

4. Modify the notification settings. To do this, in the **Event notification** section click the **Settings** link to set the required parameters. By default, the Administration Server's notification settings will be used.

   Use the **Test** button to manually send a test message. When you press this button, a test notification sending window will open. In the event of errors, detailed error information will be displayed.

Changes to the notification methods will start operating as soon as the policy settings have been saved and the policy has been applied to the administration group's client computers.

VERIFYING THE NOTIFICATION SYSTEM AND ON-DEMAND SCAN TASKS

To verify that notifications about events are being correctly distributed, and that on-demand scan tasks are working properly:

1. Try to copy the test "virus" Eicar to a protected computer. The copying operation will not be allowed if the real-time file system protection is working correctly. You will be notified that the virus was detected, and a corresponding record will appear in the **Events** folder of the console tree's top level.

2. Stop the file system real-time protection on the client computer, and copy the Eicar "virus" to the client computer. Now re-enable the file system real-time protection.

3. Start the group task which scans the client computer. The test "virus" will be detected during the task. You will be notified about the detected virus, and a corresponding record will appear in the console tree in the **Event and computer selections** → **Events** → **Recent events** folder.

The test "virus" IS NOT A VIRUS, and does not contain any code which may harm your computer. However, most manufacturers' anti-virus products identify this file as a virus. You can download the test "virus" from the official EICAR website at http://www.eicar.org/anti_virus_test_file.htm.

RECEIVING REPORTS

Based on data stored in the Kaspersky Administration Kit event log on the Administration Server, in the **Reports and notifications** folder of the console tree, you can view reports which summarize the status of anti-virus protection. The **Statistics** tab displays information under several headings: **Protection status**, **Deployment**, **Updates**, **Anti-virus statistics** and **General information**. Each section contains a set of information panels containing diagrams, graphs or text descriptions. The set of panels and their appearance can be changed using the button  .

You can also create more detailed reports, by using templates made earlier. To do this, in the **Reports and notifications** folder, go to the required report template or select the **Reports** tab in the task pane and press the link with the name of the required report.

There are several standard templates to create different types of reports about the status of anti-virus protection:

- **Kaspersky Lab software version report**.
- **Viruses report**.
- **Most infected computers report**.
- **Incompatible applications report**.
- **Users of infected computers report**.
- **Protection coverage report**.
- **Report on application registry**.
- **Protection status report**.
- **License usage report**.
- **Anti-virus database usage report**.
- **Errors report**.

For example, if you create a report on the level of virus activity, you will see information about all viruses detected by Kaspersky Administration Kit.

Additional reports are also available. They can be viewed by selecting the required report template in the console tree in the **Reports and notifications** folder. You can also create custom report templates (for more details see the Kaspersky Administration Kit Reference Guide).

CONFIGURING THE AUTOMATIC INSTALLATION OF APPLICATIONS

To automatically install applications on new computers as they are added to an administration group:

1. Open the properties window of the required administration group.
2. Select the **Automatic installation** tab.
3. Specify the installation packages to be installed on new computers, by checking the boxes beside the names of the required applications' installation packages, and press the **OK** button.

Group tasks will be created which will run on the client computers immediately after they are added to the administration group.

DAILY TASKS

To track the status of anti-virus protection, you are advised to monitor the following on a daily basis:

- the current status of the anti-virus protection in the network (see section "Viewing of the current status of anti-virus protection" on page 15);
- report about viruses found in the network (see section "Viewing report about viruses found" on page 15);
- information about important events in the operation of anti-virus applications (see section "Viewing information about important events" on page 16).

VIEWING THE CURRENT STATUS OF ANTI-VIRUS PROTECTION

The general status of the anti-virus protection can be tracked in the task pane of the **Administration Server – <Computer name>**. The information panels in this node display general information about the status of the application's different areas of functionality:

- deployment of protection on networked computers;
- creation of the administration group structure, containing the managed computers;
- operation of protection on client computers;
- client computer scans;
- updating of application databases and application modules;
- operation of monitoring and notifications.

Using the stop-light icons located in the information panels, you can quickly evaluate the status of anti-virus protection. If the icon is green, all required tasks related to this area of functionality have already been completed. If the icon is yellow or red, this area of functionality requires attention, and action may be required.

In addition to the color indication, each section contains a short description of the status or problem, as well as links which you can use to execute the main tasks.

For more detailed information about the status of anti-virus protection, please refer to the **Reports and notifications** folder.

VIEWING THE REPORT ON DETECTED VIRUSES

To view a summary of the viruses found, switch to the **Reports and notifications** folder and in the **Statistics** tab of the results pane select the **Anti-virus statistics** section. A summary of activity during the previous 24 hours will be displayed in the information panels by default:

- A history of virus activity.
- The most frequent viruses.
- Which computers were infected most often.
- Users on whose computers most virus are detected.

To view detailed information about the viruses found in the network, select the **Reports** tab, and in the **Basic reports** section click the link with the name of the required report, from this list:

- **Viruses report**.
- **Most infected computers report**.
- **Users of infected computers report**.

When you select the required report, in the results pane, information collected since the installation of Administration Server will be displayed in detail.

You can specify the time interval for which the report will be compiled, as well as the set of displayed fields (for details refer to the Kaspersky Administration Kit Reference Guide).

VIEWING INFORMATION ABOUT IMPORTANT EVENTS

To view information about important events in the operation of administered applications, select the **Event and computer selections** → **Events** folder of the console tree. In the **Preset selections** section in the task pane, click its corresponding link to go to the required event selection.

To view the latest events, use the **Recent events** link. A table will be displayed containing detailed information about each event. By default, all events that occurred during the previous seven days will be displayed.

You can view important events by using the **Critical events**, **Functional failures** and **Warnings** links.

You can create a custom event selection (for more details refer to the Kaspersky Administration Kit Reference Guide).

PERIODIC TASKS

Some additional tasks must be performed occasionally while administering the anti-virus protection system, including:

- Configuring policies for the application (on page 16).
- Configuring anti-virus application settings (on page 16).
- Printing and saving reports (on page 17).
- Backing up Administration Server data (on page 17).

For the full list of available tasks, please refer to the Kaspersky Administration Kit Administrator's Guide, Deployment Guide, and Reference Guide.

CONFIGURING POLICIES FOR THE APPLICATION

To configure an Administration Kit policy for an anti-virus application, which will be applied to computers within the current administration group:

1. Select a policy for the anti-virus application in the **Policies** folder in the administration group.
2. In the task pane in the **Actions** section, click the **Edit policy** link to go to the policy settings configurations.
3. In the window that opens, configure the policy settings.

When the settings have been saved, the policy will be applied to all computers in the administration group.

CONFIGURING ANTI-VIRUS APPLICATION SETTINGS

General settings of the application for all computers of the administration group are configured using policies (see section "Configuring policies for the application" on page 16). You can also modify the settings for the anti-virus application on a specific client computer.

To modify the settings for the anti-virus application on a specific client computer:

1. In the console tree, select the **Client computers** folder in the administration group, and open the specific client computer's properties window.
2. Select the **Applications** tab.
3. Select the required application, and press the **Properties** button.
4. Modify the application settings as required.

If a setting cannot be edited, it means that it is "locked" ( ) in the policy for this application.

After you save the settings, they will be applied to the client computer.

PRINTING AND SAVING REPORTS

Kaspersky Administration Kit can print brief reports, and save complete reports in the following formats: HTML page, Microsoft Excel file or PDF document.

- *To print a brief report:*

  1. In the console tree, select the **Reports and notifications** folder.
  2. On the **Statistics** tab in the results pane, select the required information section.
  3. Press the button .

- *To save a full report:*

  1. In the **Reports and notifications** folder of the console tree, select the required report template.
  2. In context menu of the report template, select the **Save** command and follow the wizard's instructions.

After saving a report in this way, it can be viewed and printed later using the appropriate application for the file format.

BACKING UP ADMINISTRATION SERVER DATA

The Quick Start Wizard creates an Administration Server backup copy creation task (see section "Initial anti-virus protection configuration" on page 9). By default, a backup copy is created daily on the computer on which the Administration Server is installed, in the Backup sub-folder of the application's installation folder.

To manually create a backup copy of the Administration Server data manually, in the console tree, select the **Kaspersky Administration Kit tasks** folder select the required task and click the **Run the task** link in the task pane.

UPGRADING FROM KASPERSKY ADMINISTRATION KIT 6.X TO VERSION 8.0

This section discusses how to upgrade from Kaspersky Administration Kit version 6.x to version 8.0. Some issues related to upgrading were partly discussed in previous sections. This section contains a complete description of the upgrade process.

A typical upgrade scenario is as follows:

1. A backup copy of the installed Administration Server data is created for the previous version of Kaspersky Administration Kit, using the **klbackup** utility. This utility is included in the Kaspersky Administration Kit installation package, and after the installation of the Administration Server it is located in the root of the installation folder.

2. The Administration Server and Administration Console 8.0 are installed in the corporate network. These components can be installed either on the same computer or on different computers.

   Administration Server can be installed on a computer which is already running the previous version of Administration Server, all data and settings of the previous version of the Server and / or of the Administration Console will be preserved and available in the new version.

   If Administration Server version 8.0 is installed on a different computer, the previous version's settings and data can be restored using the data backup and restoration utility klbackup.

3. Initial configuration of the anti-virus protection will be performed, if the settings were not transferred from the previous version of Administration Server.

4. The administration group structure will be created.

5. Computers will be selected for which Kaspersky Anti-Virus will be upgraded to version 6.0 MP4.

6. A remote installation task to install version 6.0 MP4 will be created for the selected computers. Installation packages created automatically during the installation of Kaspersky Administration Kit will be used.

7. The remote installation task will be started, and Kaspersky Anti-Virus version 6.0 MP4 will be installed on the selected computers. This will uninstall older versions of anti-virus applications, and install the new version.

8. Computers on which Kaspersky Anti-Virus applications version 6.0 MP4 were installed, will be added to the logical structure of the Administration Server 8.0.

Gradually the entire anti-virus protection of the company, built on the use of the earlier versions of anti-virus applications, will be transferred under the control of Kaspersky Administration Kit 8.0.

Use the Policies and Tasks Conversion Wizard to convert policies and tasks created for earlier versions of Kaspersky Lab's applications. For more details see the Kaspersky Administration Kit Reference Guide.

CONCLUSION

The features of the Kaspersky Administration Kit administration system are much broader than the description provided in this document. This document describes a simple scenario and the tasks that will allow the reader to start using the administration system, and to deploy anti-virus protection on several computers on the network. This scenario does, however, describe all the basic actions required to ensure reliable anti-virus protection of the network:

- Deployment and configuration of the anti-virus protection administration system.
- Centralized deployment of anti-virus protection on client computers across the corporate network.
- Defining anti-virus protection policies.
- Determining and verifying the operation of database update tasks on client computers.
- Verifying the protection task operation.
- Determining and launching scan on client computers.
- Receiving notifications about critical events in the operation of the anti-virus system.
- Viewing the current status of anti-virus protection, and receiving reports.
- Backing up the Administration Server's data.

KASPERSKY LAB

Kaspersky Lab was founded in 1997. Today it is the leading Russian developer of a wide range of high-performance information security software products, including anti-virus, anti-spam and anti-hacking systems.

Kaspersky Lab is an international company. Its headquarters are in the Russian Federation and it has offices in the United Kingdom, France, Germany, Japan, the Benelux countries, China, Poland, Romania and the USA (California). A new company office, the European Anti-Virus Research Centre, has recently been established in France. Kaspersky Lab's partner network includes over 500 companies worldwide.

Today, Kaspersky Lab employs over a thousand highly qualified specialists, including 10 MBA holders and 16 PhD holders. All Kaspersky Lab's senior anti-virus experts are members of the Computer Anti-Virus Researchers Organization (CARO).

Our company's most valuable assets are the unique knowledge and collective expertise accumulated during fourteen years of continuous battle against computer viruses. Constant analysis of computer virus activities enables the company's specialists to anticipate trends in the development of malware, and to provide our users with timely and reliable protection against new types of attacks. This advantage is the basis of Kaspersky Lab's products and services. We always remain one step ahead of our competitors in delivering comprehensive anti-virus coverage to our clients.

Years of hard work have made the company one of the top anti-virus software developers. Kaspersky Lab was the first to develop many of the modern standards for anti-virus software. The company's flagship product, Kaspersky Anti-Virus®, reliably protects all types of computer systems against virus attacks, including workstations, file servers, mail systems, firewalls, Internet gateways and hand-held computers. Its easy-to-use management tools maximize the automation of anti-virus protection for computers and corporate networks. A large number of developers worldwide use the Kaspersky Anti-Virus kernel in their products, including Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India), and BorderWare (Canada).

Kaspersky Lab's customers enjoy a wide range of additional services that ensure both stable operation of the company's products, and full compliance with their specific business requirements. We design, implement and support corporate anti-virus systems. Our databases are updated every hour. We provide our users with 24-hour technical support service in several languages.

If you have any questions, comments, or suggestions, you can contact us through our dealers, or at Kaspersky Lab directly. We can always give you detailed advice by telephone or email. You will receive full and comprehensive answers to all your questions.

Kaspersky Lab official site:	http://www.kaspersky.com
Virus Encyclopedia:	http://www.viruslist.com
Anti-virus laboratory:	newvirus@kaspersky.com (only for sending archives of suspicious objects) http://support.kaspersky.ru/helpdesk.html?LANG=en (for queries to virus analysts)