

Kaspersky Administration Kit 8.0

GETTING STARTED

PROGRAM VERSION: 8.0



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.

All materials may only be duplicated, regardless of form, or distributed, including in translation, with the written permission of Kaspersky Lab.

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

Kaspersky Lab reserve 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>.

Kaspersky Lab shall not be liable for the content, quality, relevance, or accuracy of any materials used in this document for which the rights are held by third parties, or for any potential or actual losses associated with the use of these materials.

This document involves the registered trademarks and service marks which are the property of their respective owners.

Revision date: 9/14/09

© 1997-2009 Kaspersky Lab ZAO. All Rights Reserved.

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

CONTENTS

INTRODUCTION	4
OBTAINING INFORMATION ABOUT THE APPLICATION.....	5
Information sources for further research	5
Contacting the Technical Support Service	6
Discussing Kaspersky Lab's applications on the web forum	7
GETTING STARTED.....	8
Deploying anti-virus protection.....	8
Installing Kaspersky Administration Kit.....	9
Initial anti-virus protection configuration	9
Creating an administration group	11
Remote installation of anti-virus applications	11
Verifying database updates.....	12
Configuring notifications	12
Verifying the notification system and on-demand scan tasks	13
Receiving reports	13
Configuring the automatic installation of applications.....	14
Daily tasks	14
Viewing the current status of anti-virus protection.....	15
Viewing the report about detected viruses	15
Viewing information about important events.....	16
Periodic tasks	16
Configuring policies for the application.....	16
Configuring anti-virus application settings.....	16
Printing and saving reports.....	17
Backing up Administration Server data	17
UPGRADING FROM KASPERSKY ADMINISTRATION KIT 6.X TO VERSION 8.0	18
CONCLUSION	19
KASPERSKY LAB.....	20

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. Throughout this document, the word "application" unless modified refers to Kaspersky Administration Kit itself: other Kaspersky Lab anti-virus applications, installed on networked computers and managed using Kaspersky Administration Kit, are referred to as "the administered application(s)".

This document describes in detail a simple installation scenario, in which an anti-virus application is deployed on several computers running the Microsoft Windows operating system, in which all the client computers are part of a single administration group.

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

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

This document also describes how to upgrade from versions 6.x to version 8.0 of the Administration Kit.

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, 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 manage the downloading of updates to administered applications' databases and modules, and distribute them to all networked computers.
- 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** which centralizes the storage of information both about administered Kaspersky Lab applications installed in the corporate network, and about their management.

- **Network Agent** which coordinates the interaction between Administration Server and installed Kaspersky Lab applications on particular workstations or servers. This component supports all the Windows applications in Kaspersky's Open Space Security range. Separate versions of the 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 an snap-in for the Microsoft Management Console (MMC).

OBTAINING INFORMATION ABOUT THE APPLICATION

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

Kaspersky Lab provides several sources of information about the application, from which you can choose the most suitable with regard to the question's importance and urgency.

IN THIS SECTION

Information sources for further research.....	5
Contacting the Technical Support Service.....	6
Discussing Kaspersky Lab's applications on the web forum	7

INFORMATION SOURCES FOR FURTHER RESEARCH

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

- the application's page at Kaspersky Lab's website;
- the application's Knowledge Base page at the Technical Support Service website;
- the installed help system;
- the installed application 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_admin

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 help system

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

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

If you have a question about a specific application window, you can use context-sensitive help, by pressing the **Help** button or **<F1>** key while the window for which you need help is open.

Documentation

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

- **Administrator's Guide** describes the purpose, basic concepts, features and general schemes for using the Kaspersky Administration Kit.
- **Deployment Guide** describes how to install Kaspersky Administration Kit's components, and the remote installation of anti-virus applications across typical computer networks.
- **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 detailed 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, either over the phone or via the Internet. When contacting the Technical Support Service, you will need to provide information about the license for the Kaspersky Lab product that you are administering through Kaspersky Administration Kit.

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 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 in the course of 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 the *license key serial number*.

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 encountered. Specify the following in the mandatory fields:

- **Request type.** Specify the topic which reflects the general nature of the problem: 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, providing as much relevant 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 collect the necessary information (listed at <http://support.kaspersky.com/support/details>) about your computer and the installed application. 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 the forum you can view existing discussions, leave your comments, create new topics, or use the search engine for specific enquiries.

GETTING STARTED

To ensure comprehensive anti-virus protection of your company, you must:

- Deploy anti-virus protection on all computers within the network (see the section "Deploying anti-virus protection" on page [8](#)).
- Perform regular tasks (see page [14](#)), which monitor the current status of anti-virus protection.
- Periodically perform additional tasks (see section "Periodic tasks" on page [16](#)), to keep the anti-virus protection up to date, and make a timely response to any problems which arise.

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

IN THIS SECTION

Deploying anti-virus protection	8
Daily tasks	14
Periodic tasks	16

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 the client computers to them. Administration groups allow a collection of client computers to be managed 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 the notification system, which informs you of events which occur during anti-virus protection on client computers (see section "Configuring notifications" on page [12](#)).
7. Run on-demand scan tasks, and verify that the notification system is functioning correctly (see section "Verifying the notification system and on-demand scan tasks" 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

► *The Administration Kit consists of two required components, the Administration Server and the Administration Console. To install these components on the same computer:*

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

You can install Kaspersky Administration Kit 8.0 as an upgrade to an existing version 5.x or 6.x installation, without removing the existing installation. Simply run the installation on the computer on which the previous version is installed. The existing settings will be re-used by the new components.

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 run.

2. Run the executable file setup.exe from the installation CD, and follow the installation wizard's instructions.
3. Select standard installation, in which most of the settings will be determined automatically.

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

Firstly the following ancillary programs, which are required for the application's operation, will be installed on the computer if they do not already exist there:

- 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.

4. 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.

When the wizard finishes, you can start the Administration Console and configure the application (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 will open, 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

The anti-virus protection is configured using 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 icon  with such 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 downloads 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. 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.
5. 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 copied into the shared folder is displayed in the console tree, in the **Repositories / Updates** node.

6. In the wizard's final window, specify whether you want to launch the application immediately after the Quick Setup Wizard completes (see section "Remote installation of anti-virus applications" on page [11](#)).

CREATING AN ADMINISTRATION GROUP

➔ *To add a new administration group:*

1. In the console tree, select the group which will include the new group.
2. Select the **Groups** tab, and in the task pane click the **Create a subgroup** link.
3. Enter the name for the new group in the window that will open, and click **OK**.

Administration Console will open on the node of the newly created group.

4. To move client computers from the **Unassigned computers** group to the newly created administration group, click the **Add computers to the group** link on the task pane, and follow the wizard's instructions.

The group's computers will be shown in the results pane in the **Client computers** nested node.

To move a set of computers to the administration group, taking into consideration any criteria, open the context menu of the **Unassigned computers** node 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 other Kaspersky Lab's 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 **Start deployment** link.
3. In the wizard that will open, 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. The 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 the 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, the existing version of Kaspersky Anti-Virus 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** node of the administration group to which the deployment was made or select the **Network** node. Locate the required computers in the results pane, and view information about the installed applications in the **Agent/Anti-virus** column. If the column contains two plus (+) signs, both the 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** node and select the task of downloading updates to repository.
2. Open the task properties window, by selecting the **Properties** item 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 so, 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 alarms 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 **Actions** section of the task pane, click the **Configure notifications** link.

3. Select the required events and specify notification delivery methods for them. To do so, press the **Properties** button and check the boxes beside the required notification methods, in the **Event notification** section. The possibilities are:
 - Notify by email.
 - Notify through NET SEND.
 - Notify by running executable or script.
 - Notify via SNMP.

To verify that notifications are being distributed as required, it is sufficient to set notification for the **Detection of Viruses, Worms, Trojans, and Malware** and **Detection of a possibly infected object** events (see section "Verifying the notification system and on-demand scan tasks" on page [13](#)).

4. Modify the notification settings, by pressing the **Settings** link in the **Event notification** section, and specify the required settings. 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** node 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's execution. 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** node.

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

You can view reports which summarize the status of anti-virus protection, in the **Reports and notifications** node of the console tree. The reports are based on data stored in the Kaspersky Administration Kit's event log on the Administration Server. 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. To do this, select the nested node with the name of the required report template. Alternatively, select the **Reports and notifications** node in the task pane, select the **Reports** tab 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, which can be viewed by selecting the required report template. These appear as nested nodes under the **Reports and notifications** node in the console tree. 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 trace the status of anti-virus protection, you are advised to monitor the following on a daily basis:

- the current status of anti-virus protection across the network (see section "Viewing the current status of anti-virus protection" on page [15](#));
- the report on viruses detected across the network (see section "Viewing the report about detected viruses" on page [15](#));
- the report on 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 traced 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 traffic-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 possibly certain actions must be performed.

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 select the **Reports and notifications** node.

VIEWING THE REPORT ABOUT DETECTED VIRUSES

To view a summary of the viruses found, select the **Reports and notifications** node 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. The default information displayed includes:

- A history of virus activity.
- The most frequent viruses.
- Which computers were infected most often.
- Which users most frequently caused infection.

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, information collected since the installation of Administration Server will be displayed, in detail, in the results pane.

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** node of the console tree. In the task pane, select the required event selection by clicking the corresponding link in the **Predefined selections** section.

To view the latest events, click the **Recent events** link in the results pane, which will display a table containing detailed information about each event. By default, all events that occurred during the previous seven days will be displayed.

You can filter the displayed events by using the **Critical events**, **Functional failures** and **Warnings** links.

You can also create 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 **Actions** section of the task pane, click the **Edit policy** link.
3. In the window that will open, modify the application settings as required.


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

CONFIGURING ANTI-VIRUS APPLICATION SETTINGS

The general settings of administered applications for all computers of the administration group can be 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. Switch to the **Reports and notifications** node in the console tree.
2. Select the required information section, on the **Statistics** tab in the results pane.
3. Press the button .

➤ *To save a full report:*

1. Select the required report template in the **Reports and notifications** node.
2. Select the **Save** command from the context menu of the report template, 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 Administration Server is installed, in the Backup sub-folder of the application's installation folder.

To create a backup copy of the Administration Server data manually, select the **Administration Server tasks** node in the console tree, 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 existing (previous) version of Kaspersky Administration Kit, using the **klbackup** utility. This utility is included in the Kaspersky Administration Kit installation package, and after installing Administration Server it is located in the installation folder.
2. The Administration Server and Administration Console 8.0 are installed in the corporate network. These components can be installed either to the same computer or to different computers.

If Administration Server version 8.0 is installed on the 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 which were 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 the installation of 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 will be upgraded from earlier versions of anti-virus applications to use Kaspersky Administration Kit 8.0 and Kaspersky Anti-Virus 6.0 MP4 applications.

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

CONCLUSION

The features of Kaspersky Administration Kit administration system are much broader than the description provided in this document. This document describes a simple scenario and tasks that will allow the reader to start using the administration system, and to deploy anti-virus protection on several computers of the network. This scenario does describe all the major actions which are 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.
- Configuring and verifying the operation of database update tasks on client computers.
- Verifying the protection task operation.
- Determining and launching the scan task 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. Headquartered in the Russian Federation, the company 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 degree holders and 16 PhD degree 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. Thorough 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 protection against new types of attacks. This advantage is the basis of Kaspersky Lab's products and services. The company's products remain one step ahead of other vendors 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 the customer's specific business requirements. We design, implement and support corporate anti-virus systems. Kaspersky Lab's anti-virus database is updated every hour. The company provides its customers 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 will be glad to assist you, via phone or email, in any matters related to our products. 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)