

Kaspersky Security Center Web-Console

**KASPERSKY** **lab**

User Guide

# CONTENTS

ABOUT THIS GUIDE .....	5
In this document .....	5
Document conventions .....	7
KASPERSKY SECURITY CENTER WEB-CONSOLE .....	8
SOFTWARE REQUIREMENTS .....	10
APPLICATION INTERFACE .....	11
CONNECTING TO ADMINISTRATION SERVER .....	13
Preparing to connect to Administration Server .....	13
Connecting to Administration Server .....	13
NETWORK PROTECTION STATUS .....	17
Viewing information on computer status .....	17
Viewing information on the protection status on computers .....	19
Viewing information on the anti-virus application database state .....	20
MANAGING COMPUTERS .....	23
About computers. About administration groups .....	23
Viewing a list of computers .....	23
Viewing computer properties .....	25
INSTALLING ANTI-VIRUS APPLICATIONS .....	28
About installing anti-virus applications .....	28
About Update Agent .....	28
About how to publish installation packages .....	29
Remote installation mode .....	29
Installing anti-virus applications to computer acting as Update Agent .....	30
Installing anti-virus application remotely .....	33
Viewing information about the status of an anti-virus remote installation .....	39
Local installation mode .....	41
Publishing installation packages .....	41
Viewing a list of published installation packages .....	43
Cancelling publication of installation package .....	44
Installing anti-virus application by using published installation package .....	45
Installing an anti-virus application manually .....	46
WORKING WITH REPORTS .....	49
About reports .....	49
Actions on reports .....	49
Viewing reports .....	50
Exporting reports .....	51
Configuring report delivery .....	51

CHANGING YOUR ACCOUNT PASSWORD .....	54
LOGGING OFF KASPERSKY SECURITY CENTER WEB-CONSOLE .....	55
GLOSSARY .....	56
KASPERSKY LAB ZAO .....	58
INFORMATION ABOUT THIRD-PARTY CODE .....	59
C++ JSON PARSER 4.03.....	59
FCGI-2.4.1-SNAP-0910052249.....	59
ICU 4.4 (INTERNATIONAL COMPONENTS FOR UNICODE).....	60
MOD_FCGI-SNAP-0910052141.....	60
TRADEMARK NOTICES.....	62
INDEX .....	63

Dear User!

Thank you for choosing our product. We hope that this document will help you in your work and will provide answers regarding this software product.

Warning! This document is the property of Kaspersky Lab ZAO (herein also referred to as Kaspersky Lab): all rights to this document are reserved by the copyright laws of the Russian Federation, and by international treaties. Illegal reproduction and distribution of this document or parts hereof will result in civil, administrative or criminal liability by applicable law.

Reproduction or distribution of any materials in any format, including translations, is allowed only with the written permission of Kaspersky Lab.

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

Kaspersky Lab reserves the right to amend this document without additional notification. You can find the latest version of this document 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.

Document revision date: 9/20/2011


© 2011 Kaspersky Lab ZAO. All Rights Reserved.

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

# ABOUT THIS GUIDE

This document provides information and step-by-step instructions for Kaspersky Security Center Web-Console.

This guide is aimed at system administrators and other IT specialists who manage anti-virus protection in organizations that use Kaspersky Lab products through an anti-virus protection service provider. These technicians are referred to as client administrators in this guide.

If you have questions about how to use Kaspersky Security Center Web-Console, you can find answers in this User Guide and in the integrated Help system. To get Help, open the main application window and click the button .

## IN THIS SECTION

---

In this document.....	<a href="#">5</a>
Document conventions.....	<a href="#">6</a>

## IN THIS DOCUMENT

This document consists of sections with descriptions of features and instructions, glossary and index.

### **Kaspersky Security Center Web-Console (see page [8](#))**

This section contains general information about Kaspersky Security Center Web-Console, its purpose, and its architecture.

### **Software requirements (see page [10](#))**

This section lists the software that must be installed before you start using the application.

### **Application interface (see page [11](#))**

This section describes the purpose of tabs and other interface elements located on the main page of the Kaspersky Security Center Web-Console web portal.

### **Connecting to Administration Server (see page [13](#))**

This section tells you how to prepare for connection and how to connect to Administration Server by using Kaspersky Security Center Web-Console.

### **Network protection status (see page [17](#))**

This section tells you how to find information on the anti-virus protection status of network computers managed by an Administration Server to which the application is connected.

### **Managing computers (see page [23](#))**

This section provides information about your network computers and administration groups and tells you how to view lists and computer properties.

### **Installing anti-virus applications (see page [28](#))**

This section details remote and local installation of anti-virus applications on the computers in your network.

### **Working with reports (see page [49](#))**

This section describes how to perform the following operations on reports provided by the Administration Server to which the application is connected: view, print, send by email, and save report data to file.

### **Changing your account password (see page [54](#))**

This section tells you how to create a new password for your account.

### **Logging off Kaspersky Security Center Web-Console (see page [55](#))**

This section tells you how to exit the application safely.

### **Glossary**

This section explains terms used in this document.

### **Kaspersky Lab ZAO (see page [58](#))**

This section contains information on Kaspersky Lab ZAO.

### **Information on third-party code (see page [59](#))**

This section covers the third-party code used in the application.

### **Trademark notices (see page [62](#))**

This section contains information about the trademarks used in these documents and their respective owners.

### **Index**

Using this section, you can easily find the required data in the document.

## DOCUMENT CONVENTIONS

Document conventions used in this document are described in the following table.

Table 1. Document conventions

SAMPLE TEXT	DOCUMENT CONVENTIONS DESCRIPTION
<i>Note that...</i>	Warnings are highlighted in red and enclosed in frames. Warnings contain important information: for example, information related to operations critical to computer safety.
It is recommended to use...	Notes are framed in dotted-line box. Notes contain additional detail and reference information.
<b>Example:</b> ...	Example blocks have a yellow background, and the heading "Example".
<i>Update means...</i>	New terms are italic.
<b>ALT+F4</b>	Names of keyboard keys are bold and are all uppercase. Names of the keys followed by a plus sign (+) indicate a combination of keys.
<b>Enable</b>	Names of interface elements are bold; for example, input fields, menu commands, and buttons.
➡ <i>To configure a task schedule:</i>	Procedure headings are italic.
help	Text in the command line and text of messages displayed on the screen have a special font.
<IP address of your computer>	Variables are enclosed in angle brackets. Instead of a variable, the corresponding value must be entered in each case; angle brackets are omitted.

# KASPERSKY SECURITY CENTER WEB-CONSOLE

Kaspersky Security Center Web-Console is a web application designed to manage the anti-virus protection status of corporate networks that are protected by Kaspersky Lab anti-virus applications.

Using the application, you can do the following:

- Manage the anti-virus protection status of the enterprise
- Install Kaspersky Lab anti-virus applications on network computers
- View reports on anti-virus protection status
- Manage the delivery of reports to interested parties: system administrators and other IT specialists

Kaspersky Security Center Web-Console works from the service provider that provides anti-virus protection to your network. The anti-virus protection provider is responsible for application installation and maintenance. You do not have to install and run Kaspersky Security Center Web-Console on your computer to work with it. All you need is a web browser (see section "Software requirements" on page [10](#)).

The following figure shows how Kaspersky Security Center Web-Console works.

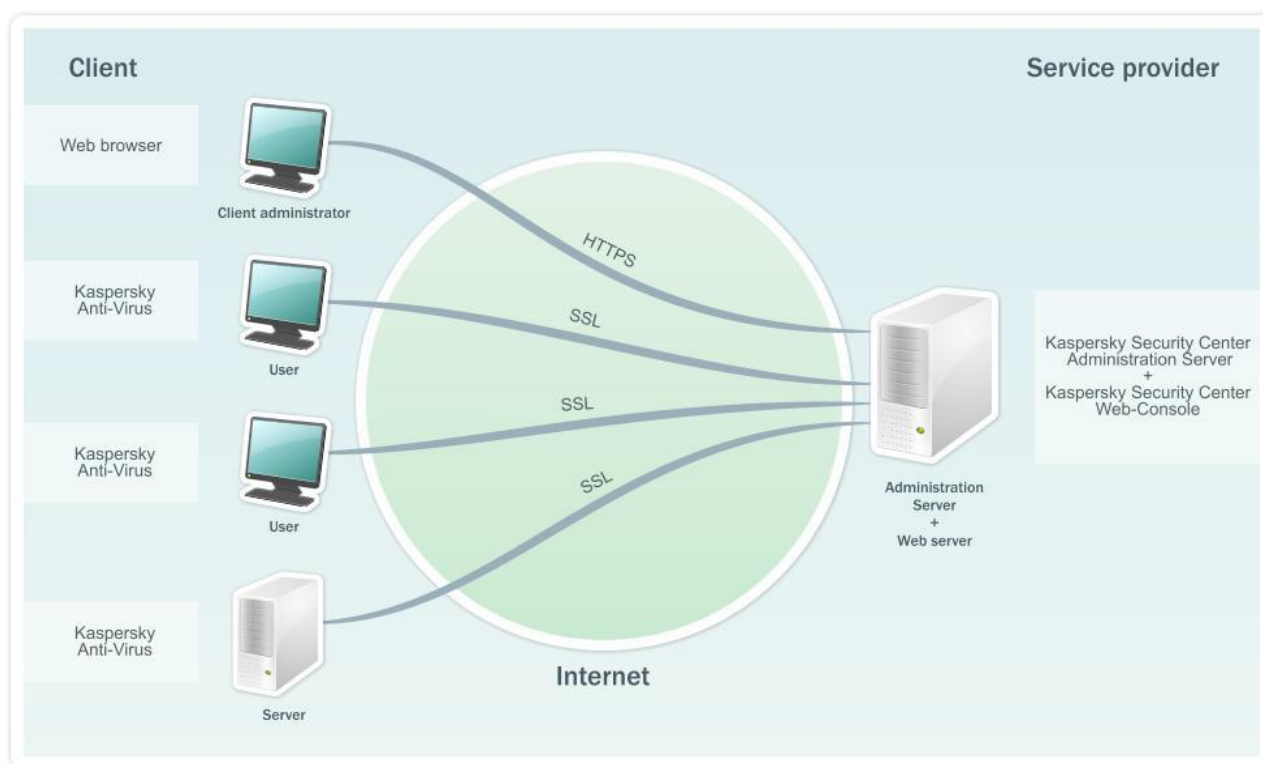


Figure 1. Operating layout

You use your web browser to connect to Kaspersky Security Center Web-Console. The web browser establishes a secure (HTTPS) connection with Kaspersky Security Center Web-Console.

Kaspersky Security Center Web-Console interacts with Kaspersky Security Center, Service Provider Edition Administration Server, which is located at the anti-virus protection service provider. Administration Server is a Kaspersky Security Center component that manages Kaspersky Lab anti-virus applications installed on your network's computers. Administration Server connects to the computers of your network over channels protected by the Secure Socket Layer (SSL) protocol.

Kaspersky Security Center Web-Console is a web interface that ensures communication between your computer and Administration Server over a web browser.

The following process describes how Kaspersky Security Center Web-Console works:

1. Use a web browser to connect to Kaspersky Security Center Web-Console, where the pages of the application web portal are displayed.
2. Use the web portal management tools to select an option to get information from Administration Server or to get an Administration Server management command. Kaspersky Security Center Web-Console performs the following operations:
  - If you choose to receive information (for example, to view a list of computers), Kaspersky Security Center Web-Console sends a request for information to the Administration Server, receives the necessary data, and sends it to the web browser in a format suitable for viewing.
  - If you choose a management command (for example, remote installation of an anti-virus application), Kaspersky Security Center Web-Console receives the command from the web browser and sends it to Administration Server. Then the application receives the result from Administration Server and sends it to the web browser in an easy-to-view format.

# SOFTWARE REQUIREMENTS

This section lists software requirements for working with Kaspersky Security Center Web-Console.

You gain access to Kaspersky Security Center Web-Console through web browser. The following are the types and versions of web browsers, and the types and versions of operating systems that you can use to work with the application.

- Microsoft® Internet Explorer® 7.0 or above on one of the following systems:
  - Microsoft Windows® XP Professional with Service Pack 2 (SP2) or later installed
  - Microsoft Windows 7.
- Firefox™ 3.6 on one of the following systems:
  - Windows operating systems:
    - Microsoft Windows XP Professional with Service Pack 2 (SP2) or later installed;
    - Microsoft Windows 7.
  - Linux® 32 bit operating systems:
    - Fedora® 10;
    - SUSE Linux Enterprise Desktop 10 with installed Service Pack 2;
    - Debian GNU/Linux 5;
    - Mandriva Corporate Desktop 4
    - Ubuntu 9.10 Server Edition
    - Ubuntu 9.10 Desktop Edition
  - Linux 64 bit operating systems:
    - Red Hat® Enterprise Linux® 5.3 server;
    - SUSE Linux Enterprise Server 10 SP2;
    - SUSE Linux Enterprise Server 11;
    - OpenSUSE Linux 11.1;
    - Ubuntu 9.10 Server Edition
- Safari 4 on one of the following operating Apple systems:
  - Mac OS X 10.4 (Tiger)
  - Mac OS X 10.5 (Leopard)
  - Mac OS X 10.6 (Snow Leopard)

# APPLICATION INTERFACE

After connection to Administration Server is established through a web browser, the main window of Kaspersky Security Center Web-Console opens (see the following figure).

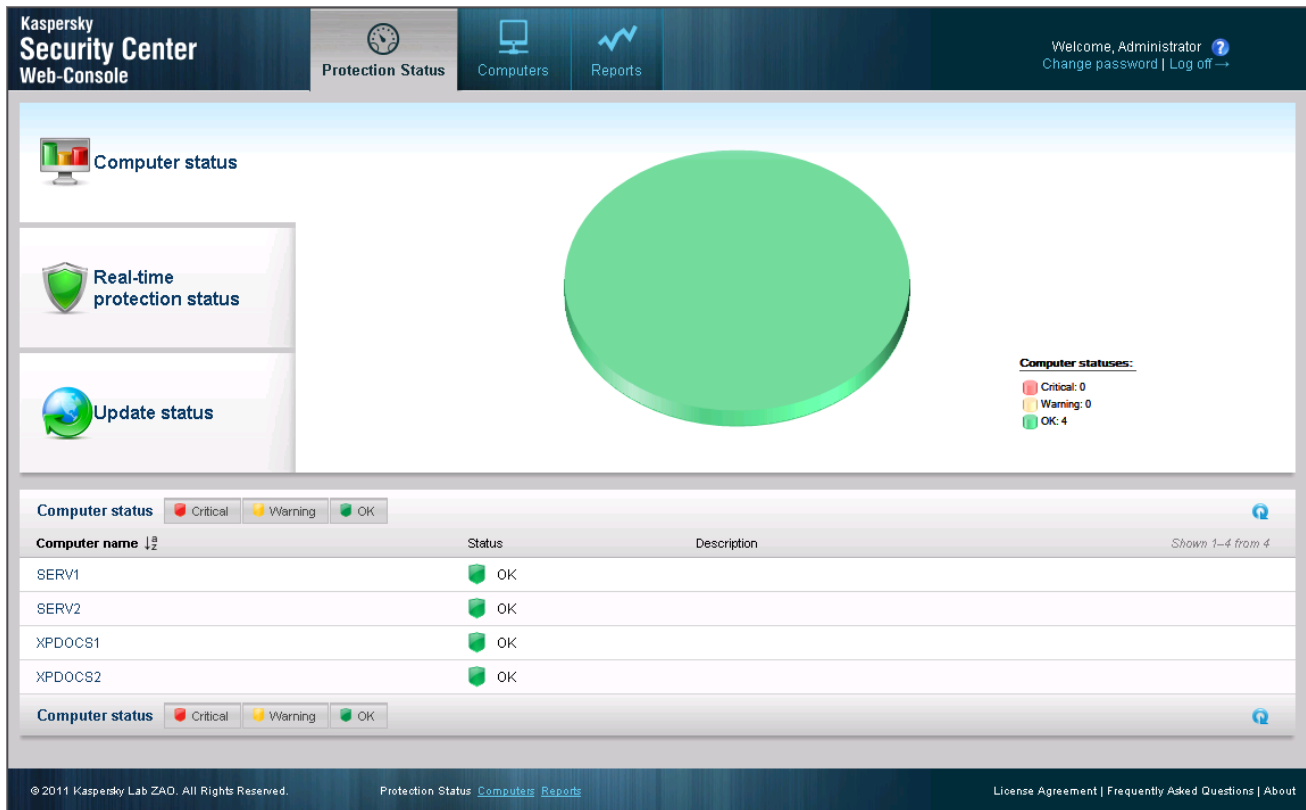


Figure 2. Main application window

The upper part of the main window contains the following interface elements:

- The **Protection Status**, **Computers** and **Reports** tabs—To access the basic application features.
- Icon —To get context-sensitive help.
- The **Change password** link—To change the password of the account.
- The **Exit** link—To exit the application.

The informational area is the principal part of the main application window. The contents of the informational area vary according to the tab that is selected:

- **Protection Status:** Contains information on the protection status of network computers. The informational area of the tab is divided into three parts. In the left part of the window you can click one of three items: **Computer status**, **Real-time protection status** and **Update status**. The results pane displays a pie chart with statistical information. The list pane in the lower part of the window displays the statuses of computers.
- **Computers:** Designed to get information on administration groups and computers. The informational area of the tab is divided into two parts. The menu contains administration groups. The results pane displays a list of computers within a selected administration group.
- **Reports:** Designed for viewing reports. The informational area of the tab is divided into two parts. The menu contains reports. The results pane displays the content of a selected report.

In the lower part of the main application window are links that duplicate the tabs.

The lower-right part of the window contains the following links:

- **End User License Agreement**—Link to the page with the End User License Agreement (EULA).
- **Frequently Asked Questions**—Link to the page with frequently asked questions (FAQ) and answers.
- **About**—Link to the application information page.

The number of links can vary depending on the configuration by the service provider's administrator. Either some links or the entire link section might not be displayed.

**SEE ALSO:**

---

Connecting to Administration Server .....	<a href="#">13</a>
Network protection status.....	<a href="#">17</a>
Managing computers.....	<a href="#">23</a>
Working with reports .....	<a href="#">49</a>
Logging off Kaspersky Security Center Web-Console .....	<a href="#">55</a>
Changing your account password .....	<a href="#">54</a>

# CONNECTING TO ADMINISTRATION SERVER

This section tells you how to prepare for connection and how to connect to Administration Server by using Kaspersky Security Center Web-Console.

## IN THIS SECTION

---

Preparing to connect to Administration Server .....	<a href="#">13</a>
Connecting to Administration Server .....	<a href="#">13</a>

## PREPARING TO CONNECT TO ADMINISTRATION SERVER

Before connecting to Administration Server, do the following: Prepare your web browser for work and collect the data required to establish the connection (an address to connect to the Administration Server and account settings: user name and password).

### Preparing the web browser

Before connecting to the Administration Server, make sure the following components are supported by your web browser:

- JavaScript
- Cookies

If support of these components is disabled, enable it. You can find information in the browser Help about how to enable support of JavaScript and cookies in your web browser.

### Receiving data for the connection

To connect to Administration Server, you must have the following data:

- Web portal address in the form `https://<Domain_name>:<Port>`
- User name
- Password

You can get this information from your service provider.

## CONNECTING TO ADMINISTRATION SERVER

➡ *To connect to Administration Server:*

1. Start the web browser.
2. In the Address bar of the web browser, enter the web portal address that you received from the service provider administrator (see section "Preparing to connect to Administration Server" on page [13](#)), and click ENTER.

If you connect to the Administration Server for the first time, your web browser will display the **License Agreement** window (see the figure below). If you have connected to the Administration Server before, the web browser will display a window asking you to enter the user name and password.

3. If you connect to the Administration Server for the first time, in the **License Agreement** window perform the following actions:
  - a. Read the License Agreement carefully. If you accept the terms, select the **I accept the terms of the License Agreement** check box.
  - b. Click the **Continue** button.

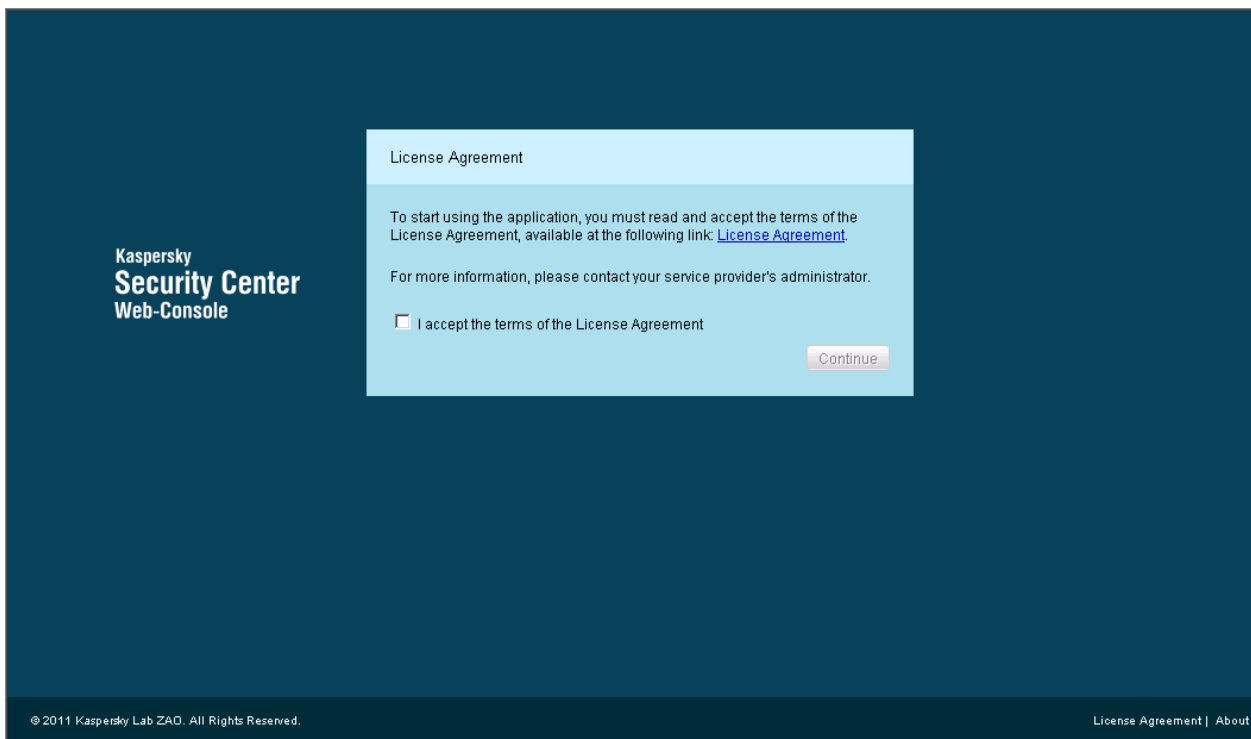


Figure 3. License Agreement

On the web portal page of the application, a dialog box opens, asking you for your user name and password (see the following figure).

4. In the **User name** text box enter your account name.

5. In the **Password** text box, enter the password of your account.

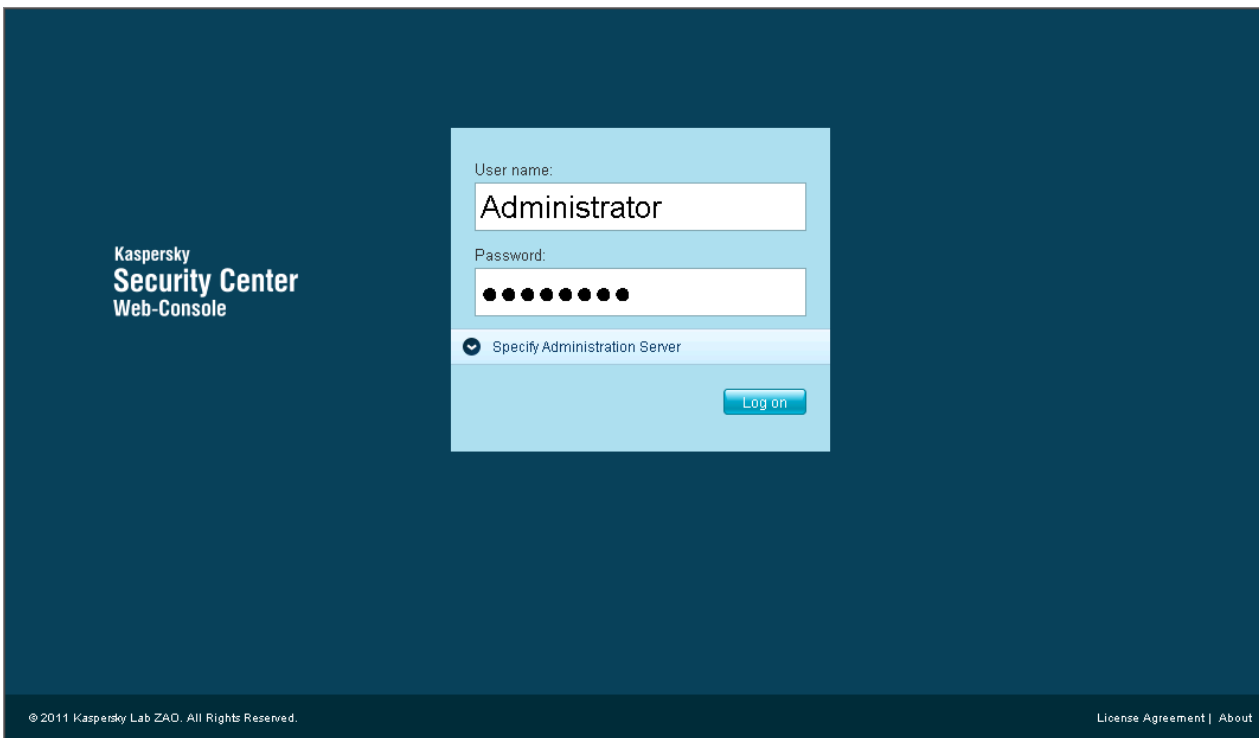



Figure 4. Entering user name and password

6. Specify an Administration Server to which you want to connect:
  - a. Open the **Specify Administration Server** drop-down section by clicking the button .

- b. In the **Administration Server** text box enter the name of Administration Server to which you want to connect (see the following figure).

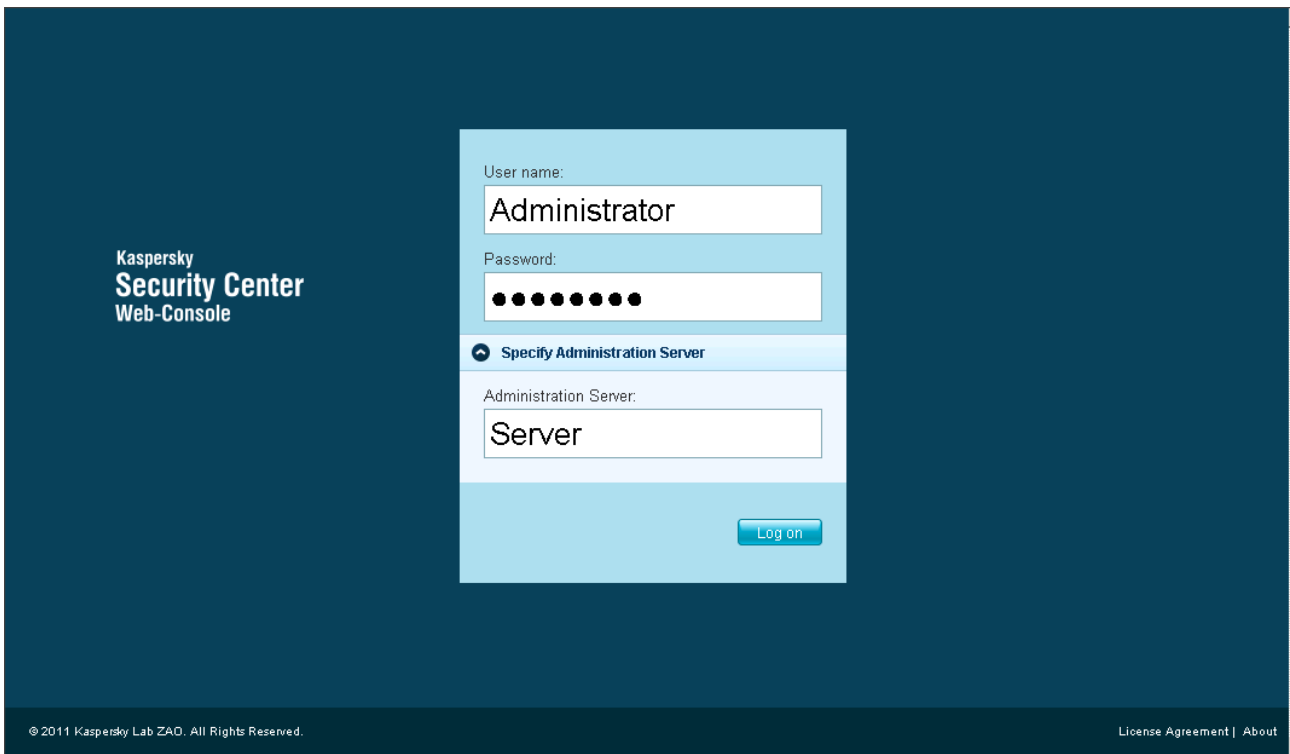


Figure 5. Selecting an Administration Server

- 7. Click the **Log in** button.

The main application window opens (see section "Application interface" on page [11](#)).

If connection to Administration Server completes with an error, to resolve this issue, contact the administrator of your service provider.

# NETWORK PROTECTION STATUS

Kaspersky Security Center Web-Console allows you to receive information about the anti-virus protection status of network computers that are managed by Administration Server.

You can receive the following information about the state of computers in your network:

- **Computer status** – information on the status of computers in your network.

A computer can have one of three statuses:

- *OK*—The computer is protected.
- *Warning*—The level of computer protection is reduced.
- *Critical*—The level of computer protection is reduced substantially.

The Administration Server assigns a status to the computer based on information about its protection status. The Administration Server assigns the *Warning* or *Critical* status to a computer if there are factors that lower the protection status of the computer (such as inactivity of an anti-virus application, out-of-date databases, or a large number of infected objects). The list of factors for *Warning* and *Critical* statuses is created by the service provider's administrator.

- **Real-time protection status**—Information on the status of a protection component in anti-virus applications installed on your network computers.
- **Update status**—Information on the database update status of an anti-virus application on your network computers.

## IN THIS SECTION

---

Viewing information on computer status.....	<a href="#">17</a>
Viewing information on the protection status on computers .....	<a href="#">19</a>
Viewing information on the anti-virus application database state .....	<a href="#">20</a>

## VIEWING INFORMATION ON COMPUTER STATUS

➔ *To view information on computers in your network:*

1. Open the main application window (see section "Application interface" on page [11](#)).
2. Click the **Protection Status** tab.

The **Computer status** item in the menu is selected (see the following figure).

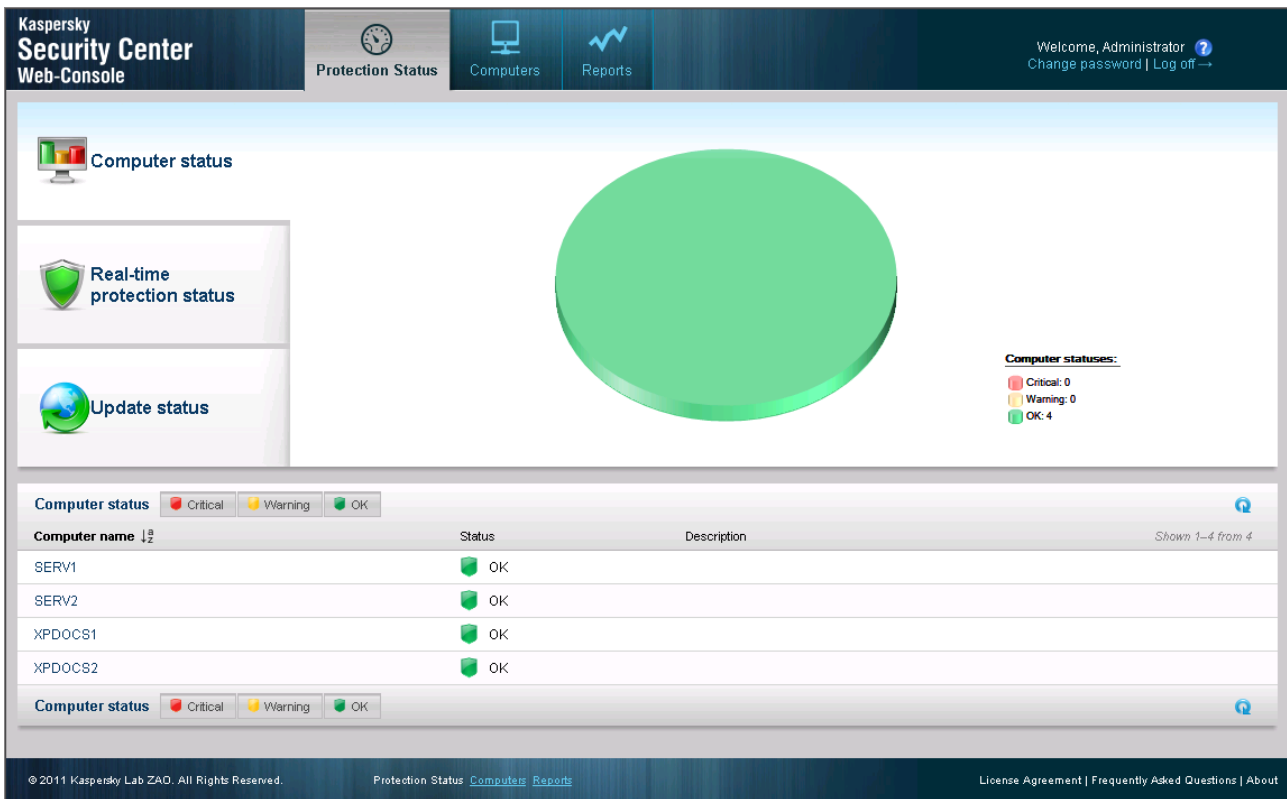


Figure 6. Computers status

The results pane displays a pie chart. It shows the numbers and percentages of computers with *Critical*, *Warning* and *OK* statuses.

The lower part of the window contains a list of computers. The list of computers contains the following information:

- **Computer name.** Name in which a computer is registered in the network.
- **Status** (*OK*, *Warning*, *Critical*). Information about computer status.
- **Description.** Messages that explain the causes of the lowered protection levels on computers that have *Warning* and *Critical* statuses (such as *Real-time protection is paused* or *The update task has not been started in more than 3 days*).

To view information about a specific computer, use the following interface elements to locate the computer in the list:

**Critical** button – Displays computers that have *Critical* status.

**Warning** button – Displays computers that have *Warning* status.

**OK** button – Displays computers that have *OK* status.

Buttons – Goes to the next / previous first / last page of the computer list.

Icon —Filters computer names in the computer list in ascending or descending alphabetical order.

Icon —Updates the computer list.

<**Computer name**> link—Goes to the <**Computer name**> properties page.

**SEE ALSO:**

About computers. About administration groups.....[23](#)  
 Viewing a list of computers.....[23](#)  
 Viewing computer properties.....[25](#)

## VIEWING INFORMATION ON THE PROTECTION STATUS ON COMPUTERS

➔ To view information about the protection status of network computers:

1. Open the main application window (see section "Application interface" on page [11](#)).
2. Click the **Protection Status** tab.
3. In the menu, click **Real-time protection status** (see the following figure).

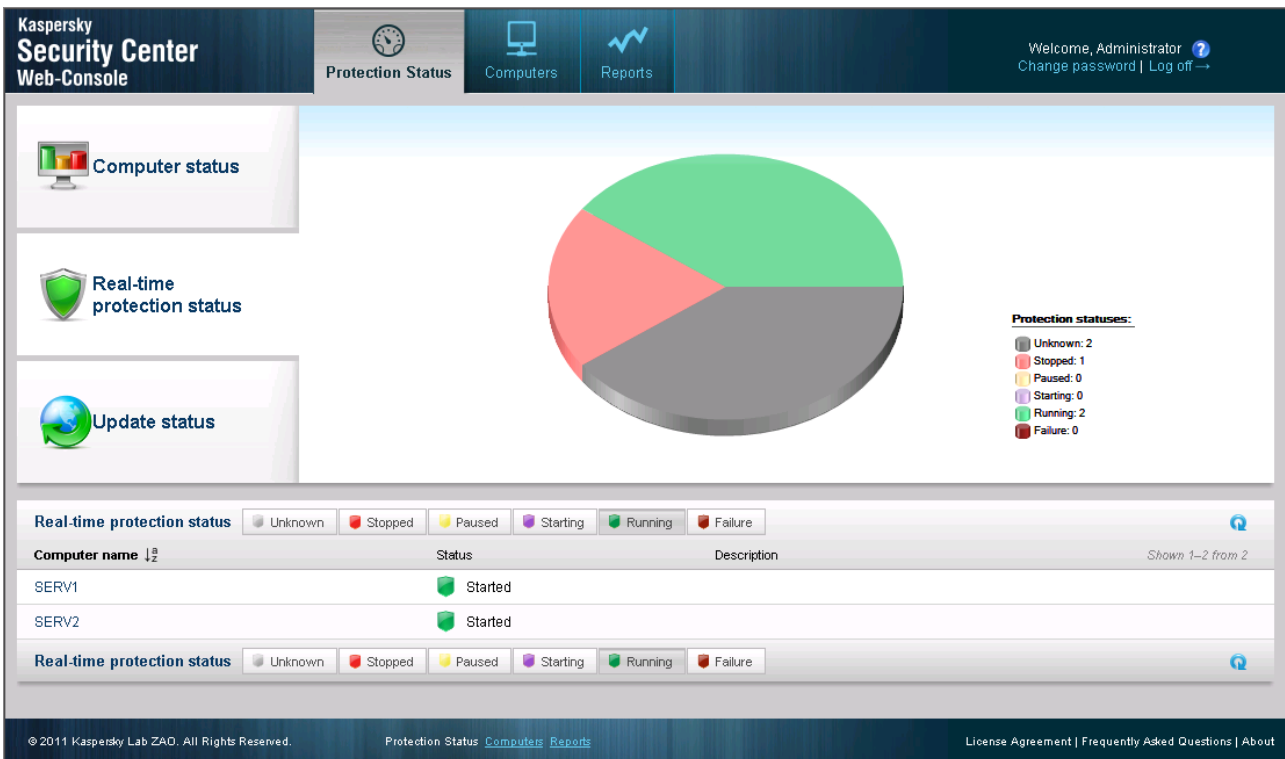


Figure 7. Real-time protection status

The results pane displays a pie chart. It contains information on the status of the protection component in the anti-virus applications installed on your network computers.

The chart shows the numbers and the percentages of computers where the component in the anti-virus application has the following statuses:

- *Unknown*

- *Stopped*
- *Paused*
- *Launching*
- *Running*
- *Failure*

The lower part of the window contains a list of computers. The list of computers contains the following information:

- **Computer name.** Name in which a computer is registered in the network.
- **Status** (*OK, Warning, Critical*). Information about computer status.
- **Description.** Messages that explain the causes of the lowered protection levels on computers that have *Warning* and *Critical* statuses (such as *The number of infected objects is too large* or *License expired*).

To view information about a specific computer, use the following interface elements to locate the computer in the list:

**Unknown** button – Displays computers that have *Unknown* protection status.


**Stopped** button – Displays computers with *Stopped* protection status.


**Paused** button – Displays computers with *Paused* protection status.


**Starting** button – Displays computers with *Starting* protection status.

**Running** button – Displays computers with *Running* protection status.

**Failure** button – Displays computers with *Failure* protection status.

Button  —Goes to next / previous first / last page of the list of computers.

Icon  —Filters computer names in the computer list in ascending or descending alphabetical order.

Icon  —Updates the computer list.

<**Computer name**> link—Goes to the <**Computer name**> properties page.

**SEE ALSO:**

---

About computers. About administration groups.....	<a href="#">23</a>
Viewing computer properties.....	<a href="#">25</a>

## VIEWING INFORMATION ON THE ANTI-VIRUS APPLICATION DATABASE STATE

➤ To view information about the database status of anti-virus application on network computers:

1. Open the main application window (see section "Application interface" on page [11](#)).
2. Click the **Protection Status** tab.

3. In the left part of the window click **Update status** (see the following figure).



Figure 8. Update status

The upper part of the section displays a bar chart. The bar chart contains information on the state of the anti-virus application on your network computers.

The bar chart displays the number of computers on which the anti-virus application databases have the following statuses:

- *Up to date*—Databases are up to date.
- *Last 24 hours*—Databases were updated during the last 24 hours.
- *Last 3 days*—Databases were updated during the last 3 days.
- *Last 7 days*—Databases were updated during the last 7 days.
- *More than a week ago*—Databases were updated more than a week ago.

The lower part of the window contains a list of computers. The list of computers contains the following information:

- **Computer name.** Name in which a computer is registered in the network.
- **Status** (*OK, Warning, Critical*). Information about computer status.
- **Description.** Messages that explain the causes of the lowered protection levels on computers that have *Warning* and *Critical* statuses (such as *Real-time protection is paused* or *The update task has not been started in more than 3 days*).

To view information about a specific computer, use the following interface elements to locate the computer in the list:


**Up to date** button – Displays computers with the *Up to date* status.


**Last 24 hours** button – Displays computers that have the *Last 24 hours* status.


**Last 3 days** button – Displays computers that have the *Last 3 days* status.

**Last 7 days** button – Displays computers that have the *Last 7 days* status.

**More than a week ago** button – Displays computers that have the *More than a week ago* status.

Button —Goes to next / previous first / last page of the list of computers.

Icon —Filters computer names in the computer list in ascending or descending alphabetical order.

Icon —Updates computer list.

**<Computer name>** link—Goes to the **<Computer name>** properties page.

**SEE ALSO:**

---

About computers. About administration groups.....	<a href="#">23</a>
Viewing computer properties.....	<a href="#">25</a>

# MANAGING COMPUTERS

This section provides information about your network computers and administration groups and tells you how to view lists and computer properties.

## IN THIS SECTION

---

About computers. About administration groups.....	<a href="#">23</a>
Viewing a list of computers.....	<a href="#">23</a>
Viewing computer properties.....	<a href="#">25</a>

## ABOUT COMPUTERS. ABOUT ADMINISTRATION GROUPS

The anti-virus protection status of your network computers is managed by Administration Server from your anti-virus protection service provider.

The computers in your network that have Kaspersky Lab applications installed are assigned to *administration groups*. Administration groups are sets of computers grouped by function and installed Kaspersky Lab applications.

By default, Administration Server contains the **Managed computers** administration group. After Kaspersky Lab applications are installed on a network computer, the computer is added to the **Managed computers** administration group. The service provider's administrator can create other administration groups and assign computers to these groups. An administration group can contain other administration groups.

Computers included in an administration group are referred to as *managed*. You can add computers in your network to the list of managed computers, to the **Managed computers** administration group. To do this, first install the Kaspersky Lab anti-virus application.

Using Kaspersky Security Center Web-Console, you can get information about managed computers from Administration Server: view list of computers and properties of managed computers.

## SEE ALSO:

---

Installing anti-virus applications.....	<a href="#">28</a>
---	--------------------

## VIEWING A LIST OF COMPUTERS

You can view lists of your network computers that are managed by Administration Server. You can view the lists of managed computers for each administration group separately.

➔ *To view a list of computers:*

1. Open the main application window (see section "Application interface" on page [11](#)).
2. Click the **Computers** tab.
3. In the left part of the window click an administration group for which you want to view a list of computers:
  - If you want to see a list of all managed computers, click the **Managed computers** group.

- If you want to view a list of managed computers in particular administration subgroup, click an administration group from the group tree located in subfolder of **Managed computers**.

A list of computers from the selected administration group is displayed (see the following figure).

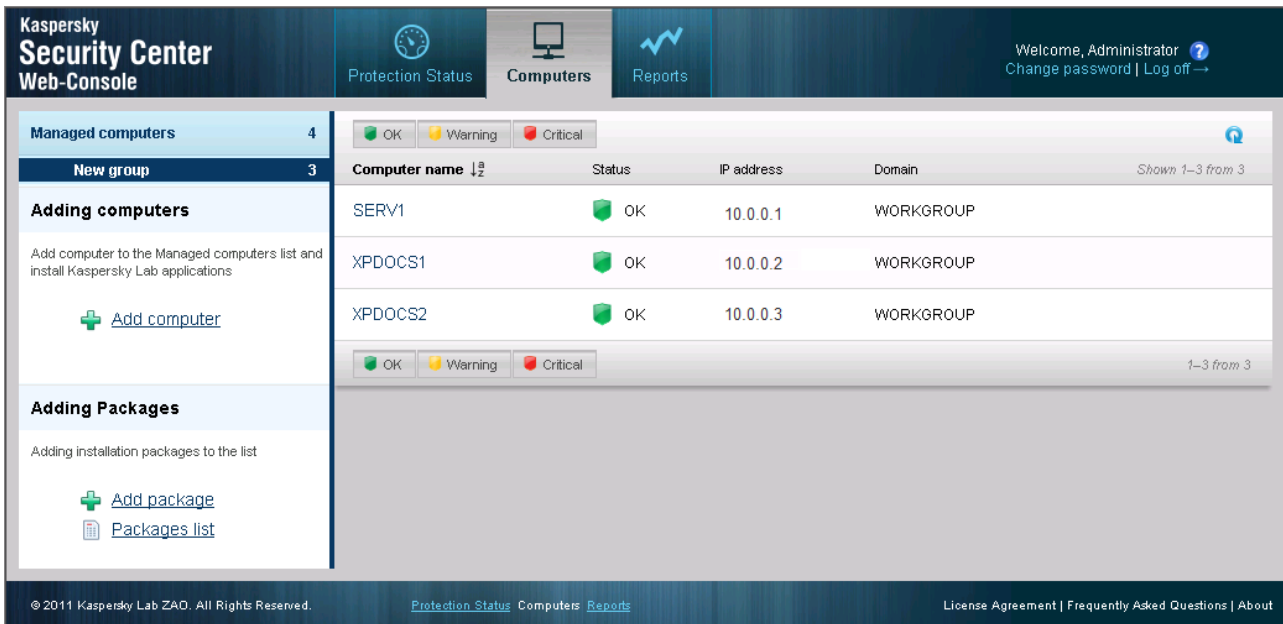


Figure 9. Viewing a list of computers

The list of computers contains the following information:

- **Computer name.** Name in which a computer is registered in the network.
- **Status.** Computer status.
- **IP address.** Network address of the computer.
- **Domain.** Name of the network domain where the computer is registered.

To view information about a specific computer, use the following interface elements to locate the computer in the list:

**Critical** button – Displays computers that have *Critical* status.

**Warning** button – Displays computers that have *Warning* status.

**OK** button – Displays computers that have *OK* status.

Buttons – Goes to the next / previous first / last page of the computer list.

Icon – Filters computer names in the computer list in ascending or descending alphabetical order.

Icon – Updates the computer list.

<**Computer name**> link—Goes to the <**Computer name**> properties page.

**SEE ALSO:**

About computers. About administration groups.....	<a href="#">23</a>
Network protection status.....	<a href="#">17</a>

## VIEWING COMPUTER PROPERTIES

➔ To view computer properties:

1. Open the main application window (see section "Application interface" on page [11](#)).
2. Click the **Computers** tab.
3. In the left part of the window, in the administration groups list, select the administration group where your computer is located.

The right part of the window displays the list of computers for the selected administration group.

4. In the list of computers, find the computer whose properties you want to view. If necessary, use navigation and filtering tools.
5. Click the **<Computer name>** link to open its properties (see the following figure).

The screenshot shows the Kaspersky Security Center Web-Console interface. The top navigation bar includes 'Protection Status', 'Computers', and 'Reports' tabs. The main content area is titled 'Managed computers' and displays the properties of a computer named 'SERV2'. The left sidebar shows the computer's name, a 'DK' status, and 'Real-time protection status: Started'. The right main panel is divided into two sections: 'Computer Info' and 'Applications'. The 'Computer Info' section lists various details such as Domain (WORKGROUP), Network name (SERV2), Domain name (serv2.domain.local), IP address (10.0.0.4), Connection IP address (10.0.0.4), and Operating system (OS) (Microsoft Windows Vista). The 'Applications' section lists the 'Kaspersky Security Center Network Agent' with its version (9.0.2771) and the date of the last connection to the server (September 15-th 2011 07:57).

Figure 10. Viewing computer properties

The computer property information appears in two categories.

The left part of the window contains the following computer properties:

- Name in which a computer is registered in the network.
- Computer status.

- Warnings that contain information about the causes of decreased computer anti-virus protection, such as out-of-date anti-virus databases or large number of infected objects on computer. Warnings are displayed if the computer protection status is *Warning* or *Critical*.
- **Group.** Name of the administration group to which the computer belongs.
- **IP address.** Network address of the computer.
- **Real-time protection status.** Status of real-time protection of the computer.

In the right part of the window are two categories that each contain information related to computer properties: **Computer information** and **Applications**.

The **Applications** section is displayed only if there are Kaspersky Lab applications installed on this computer.

The **Computer information** section contains information on the following computer properties:


- **Domain.** Name of the network domain where the computer is registered.
- **Network name.** Name in which a computer is registered in the network. The network name matches the computer name that is displayed in the left part of the window.
- **Domain name.** Full computer domain name, in the format <Computer\_name>.<Domain\_name>.
- **IP address.** Network address of the computer.
- **IP connection address.** Network address for the connection to Administration Server. For example, if you connect to Administration Server by means of a proxy server, enter the proxy server address.
- **Operating system (OS).** Type of operating system installed on the computer.
- **Date of last update.** Date of last update of applications or Kaspersky Lab anti-virus databases on the computer.
- **Visible.** Date and time from which the computer is visible in the network.
- **Last connection to Server date.** Date and time of last connection to Administration Server.


The **Applications** section contains information about Kaspersky Lab anti-virus applications installed on the computer.


The **Applications** section contains the following information:

- **Application name.** Full name of the application.
- Application properties, such as the application version or the date of the last update. The list of application properties is displayed after the application name. Each application has its own set of properties.

To view computer properties, you can use the following interface elements:

Icon —Refreshes the page that contains computer properties.

Icon —Opens an information section that contains computer or application properties.

Icon —Closes information section that contains computer or application properties.

**SEE ALSO:**

---

About computers. About administration groups.....	<a href="#">23</a>
Viewing a list of computers.....	<a href="#">23</a>

# INSTALLING ANTI-VIRUS APPLICATIONS

This section details remote and local installation of anti-virus applications on the computers in your network.

## IN THIS SECTION

---

About installing anti-virus applications .....	<a href="#">28</a>
About Update Agent.....	<a href="#">28</a>
About how to publish installation packages.....	<a href="#">29</a>
Remote installation mode.....	<a href="#">29</a>
Local installation mode.....	<a href="#">41</a>

## ABOUT INSTALLING ANTI-VIRUS APPLICATIONS

Using Kaspersky Security Center Web-Console you can install anti-virus applications on your network computers. The list of anti-virus applications available for installation is created and maintained by your service provider's administrator.

There are two ways to install an anti-virus application:

- *Remote installation* (referred to as remote installation mode);
- *Local installation* (referred to as local installation mode).

Anti-virus applications are stored on Administration Server as installation packages. *Installation packages* – are sets of files required to install Kaspersky Lab applications remotely. Remote installation allows you to install an anti-virus application on several computers in your network at once. Remote installation mode involves starting and managing the installation process through the application's web portal.

You can also install anti-virus applications locally on computers of your network. For example, you may need to install an anti-virus application locally, if remote installation failed on one or more computers. You can give permissions to your network's users to install applications locally on their computers.

## SEE ALSO:

---

Local installation mode.....	<a href="#">41</a>
Remote installation mode.....	<a href="#">29</a>
Installing anti-virus application remotely.....	<a href="#">33</a>
Installing an anti-virus application manually .....	<a href="#">46</a>

## ABOUT UPDATE AGENT

Before you install anti-virus applications on the computers of your network in remote installation mode, you must assign to one of these computers the *Update Agent* status. Update Agent is a computer that acts as intermediate sources for the distribution of updates for anti-virus applications and distribution of installation packages within a group.

This Update Agent should:

- be turned on permanently or most time;
- have direct access to the Internet and other computers that belong to the same administration group.

You should install Kaspersky Anti-Virus on the computer that acts as Update Agent.

After you assigned the Update Agent status to one of the computers in your network and installed Kaspersky Anti-Virus to it, you can install anti-virus applications to other network computers in remote installation mode.

#### SEE ALSO:

About computers. About administration groups.....	<a href="#">23</a>
Installing anti-virus applications to computer acting as Update Agent.....	<a href="#">30</a>

## ABOUT HOW TO PUBLISH INSTALLATION PACKAGES

You can allow the users of your network to install Kaspersky Lab anti-virus applications on their computers independently. To do this, you can publish anti-virus applications installation packages by using Kaspersky Security Center Web-Console. A published installation package is a prepared executable file designed to install an anti-virus application with preconfigured settings. To install an anti-virus application by using a published installation package, download it to client computer and run. After you run a published installation package, an anti-virus application is installed automatically. A list of installation packages that can be published is created and maintained by your service provider's administrator.

Published installation packages are stored on Administration Server. Kaspersky Security Center Web-Console provides links for published installation packages. You can send these links to the users of your network. After the user receives a link to published installation package (for example, by email), they can download it to their computer and install an anti-virus application. To be able to do this, a local or domain account should have rights for installing applications on this computer.

You can cancel publishing installation package; for example, if they are outdated. If you cancel the publication, the installation package will be removed from the Administration Server. After you cancel the publication, the link expires. The package becomes unavailable.

#### SEE ALSO:

Cancelling publication of installation package .....	<a href="#">44</a>
Viewing a list of published installation packages.....	<a href="#">43</a>
Publishing installation packages .....	<a href="#">41</a>

## REMOTE INSTALLATION MODE

The remote installation mode allows you to install anti-virus applications to several computers in your network.

To make the remote installation mode available, assign one of network computers an Update Agent status and install Kaspersky Anti-Virus on it. After this, you can start remote installation of an anti-virus application on computers of your network.

Kaspersky Security Center Web-Console installs anti-virus applications in the background. During remote installation, you can use other application's features and view information about the status of the remote installation for each computers on which it has been started.

**IN THIS SECTION**

---

Installing anti-virus applications to computer acting as Update Agent.....[30](#)

Installing anti-virus application remotely.....[33](#)

Viewing information about the status of an anti-virus remote installation.....[39](#)

**INSTALLING ANTI-VIRUS APPLICATIONS TO COMPUTER ACTING AS UPDATE AGENT**

After you select a computer that will be used as Update Agent, install Kaspersky Anti-Virus on it from the distribution package of Kaspersky Security Center Web-Console. The first setup of Kaspersky Anti-Virus is performed locally. After you install Kaspersky Anti-Virus to local computer, this computer becomes Update Agent automatically. Update Agent allows you to install and manage anti-virus applications on remote computers.

◆ *To install anti-virus application to a computer acting as an Update Agent:*

1. Open the main application window (see section "Application interface" on page [11](#)).
2. Click the **Computers** tab.
3. Click the **Add computer** link in the pane to the left to start the Application Setup Wizard.

The Application Setup Wizard opens with a Welcome page (see the following figure).

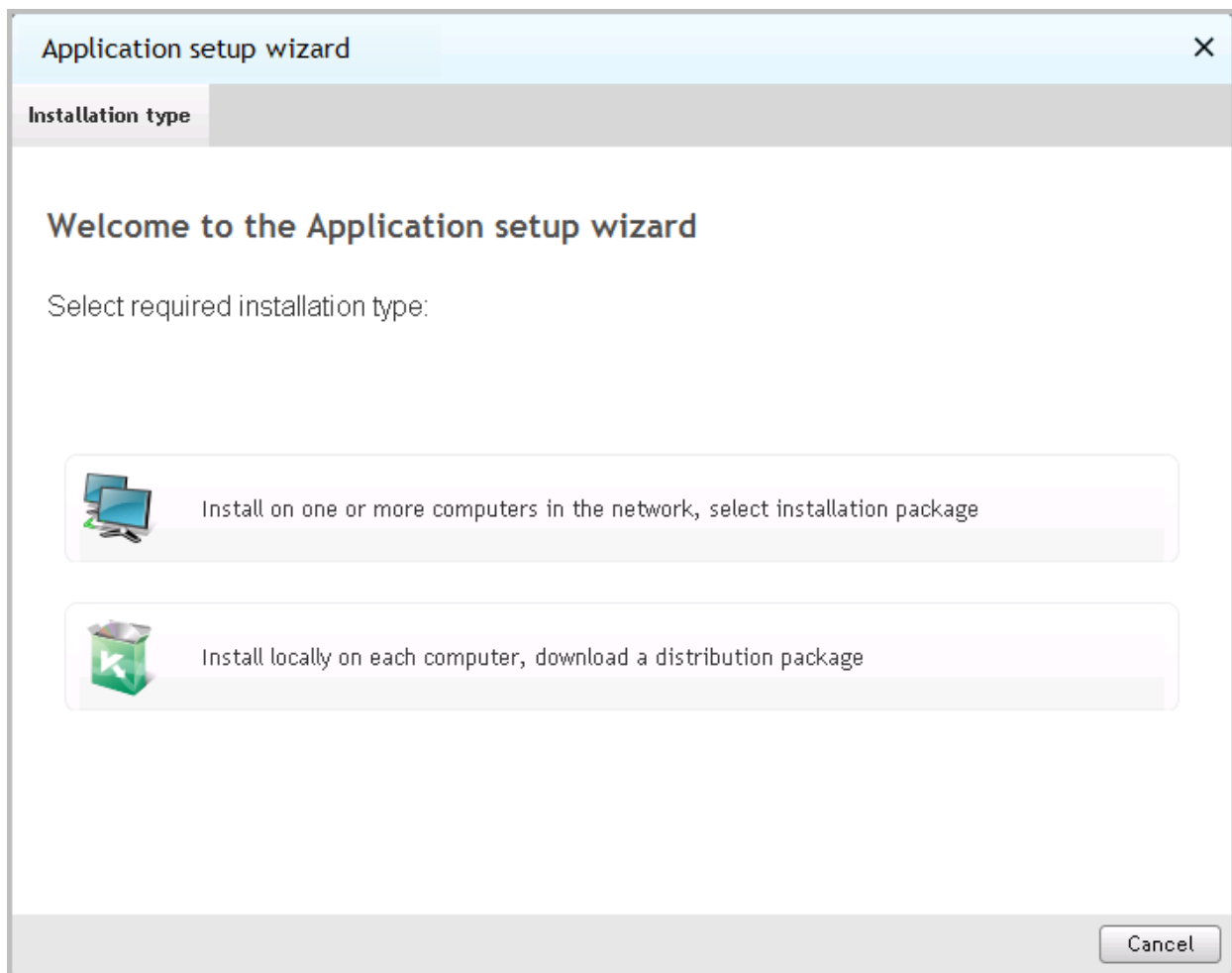


Figure 11. Application Setup Wizard. Welcome page

4. Click the button **Install locally on each computer, download a distribution package**.

The **Select a distribution package to download** window opens (see the figure below).

If no published installation packages are discovered, you will be asked to publish installation packages (see section "Publishing installation packages" on page 41). After installation packages are published, the installation of anti-virus application will continue.

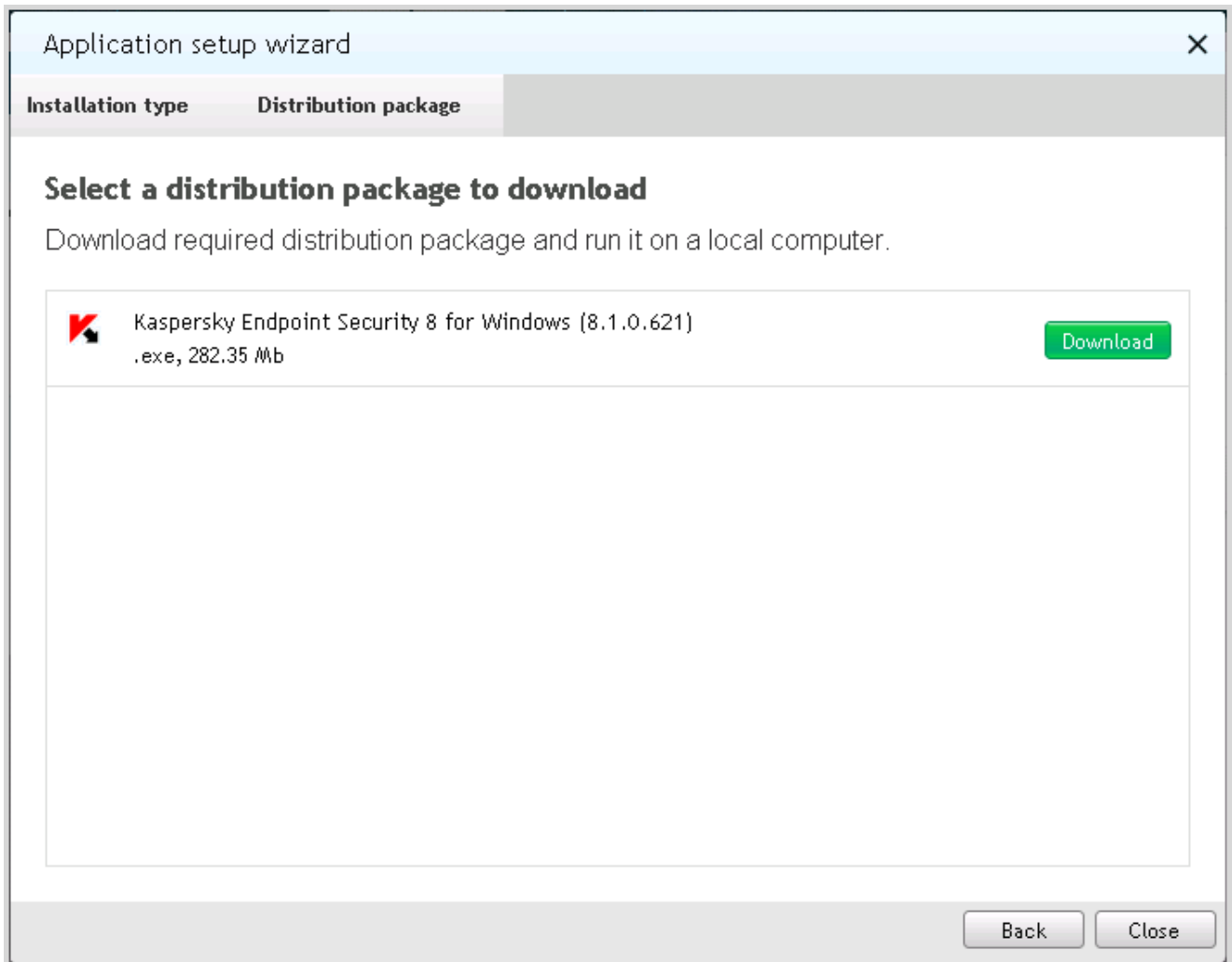


Figure 12. Application Setup Wizard. Downloading an installation package

5. Download Kaspersky Anti-Virus distribution package and click the **Download** button next to the application name.
6. Click the **Finish** button. The Application Setup Wizard closes.
7. Copy the Kaspersky Anti-Virus distribution package to the computer of your network that you assigned as Update Agent, using external media or by network. Install Kaspersky Anti-Virus from distribution package using the setup wizard's instructions.

After Kaspersky Anti-Virus is successfully installed, this computer is added to the **Managed computers** administration group. In the setup wizard, the option of remote installation of anti-virus applications becomes available.

The computer acting as Update Agent is displayed in the computer list the next time you log on to Kaspersky Security Center Web-Console portal or update the list.

If during installation an error message is displayed, contact your service provider's administrator.

## INSTALLING ANTI-VIRUS APPLICATION REMOTELY

➤ To install an anti-virus application on your network computers in remote installation mode:

1. Open the main application window (see section "Application interface" on page [11](#)).
2. Click the **Computers** tab.
3. Click the **Add computer** link in the pane to the left to start the Application Setup Wizard.

The Application Setup Wizard opens with a Welcome page (see the following figure).

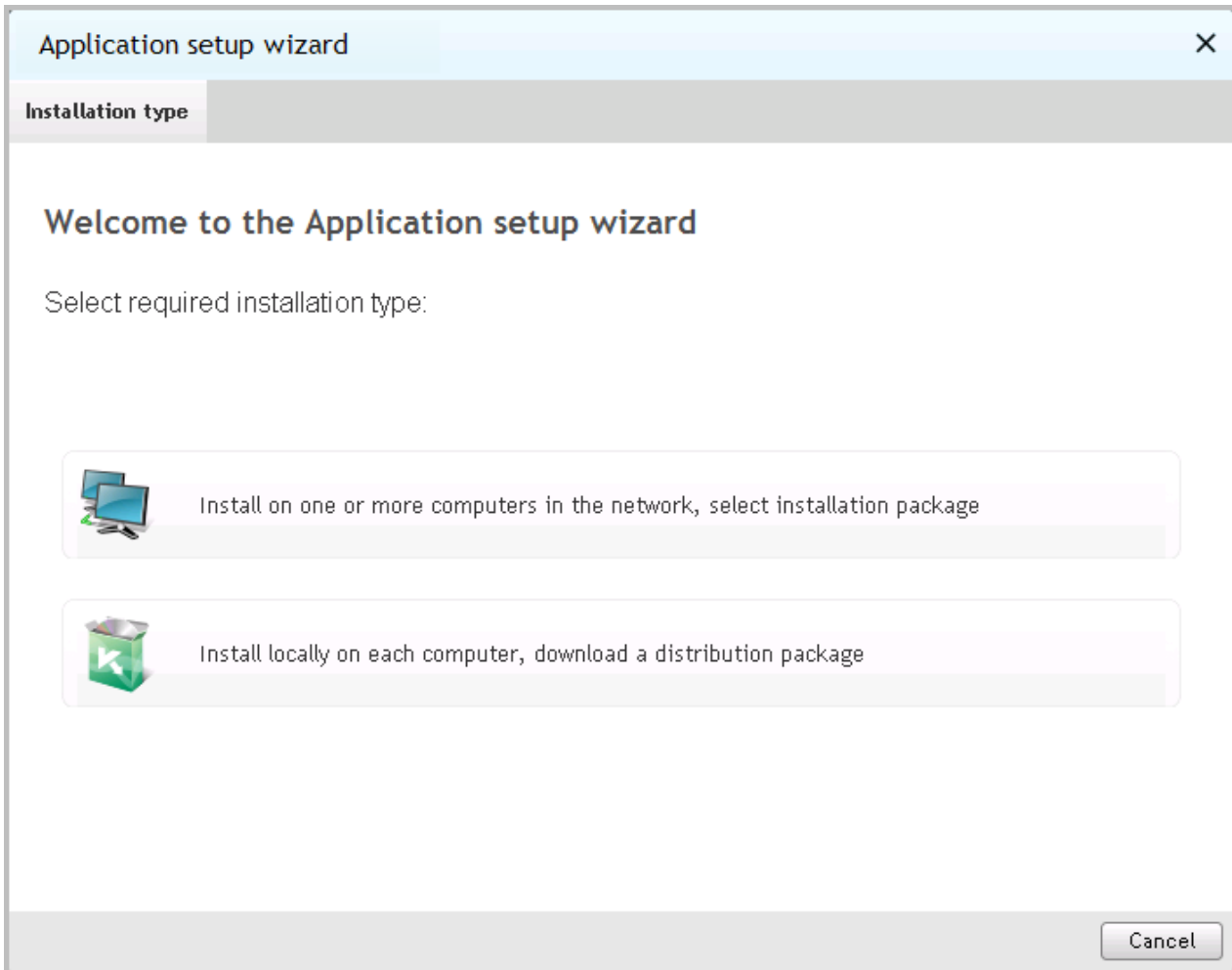


Figure 13. Application Setup Wizard. Welcome page

4. Click the button **Install on one or more computers in the network, select installation package**.

The **Selecting installation package** window opens (see the following figure).

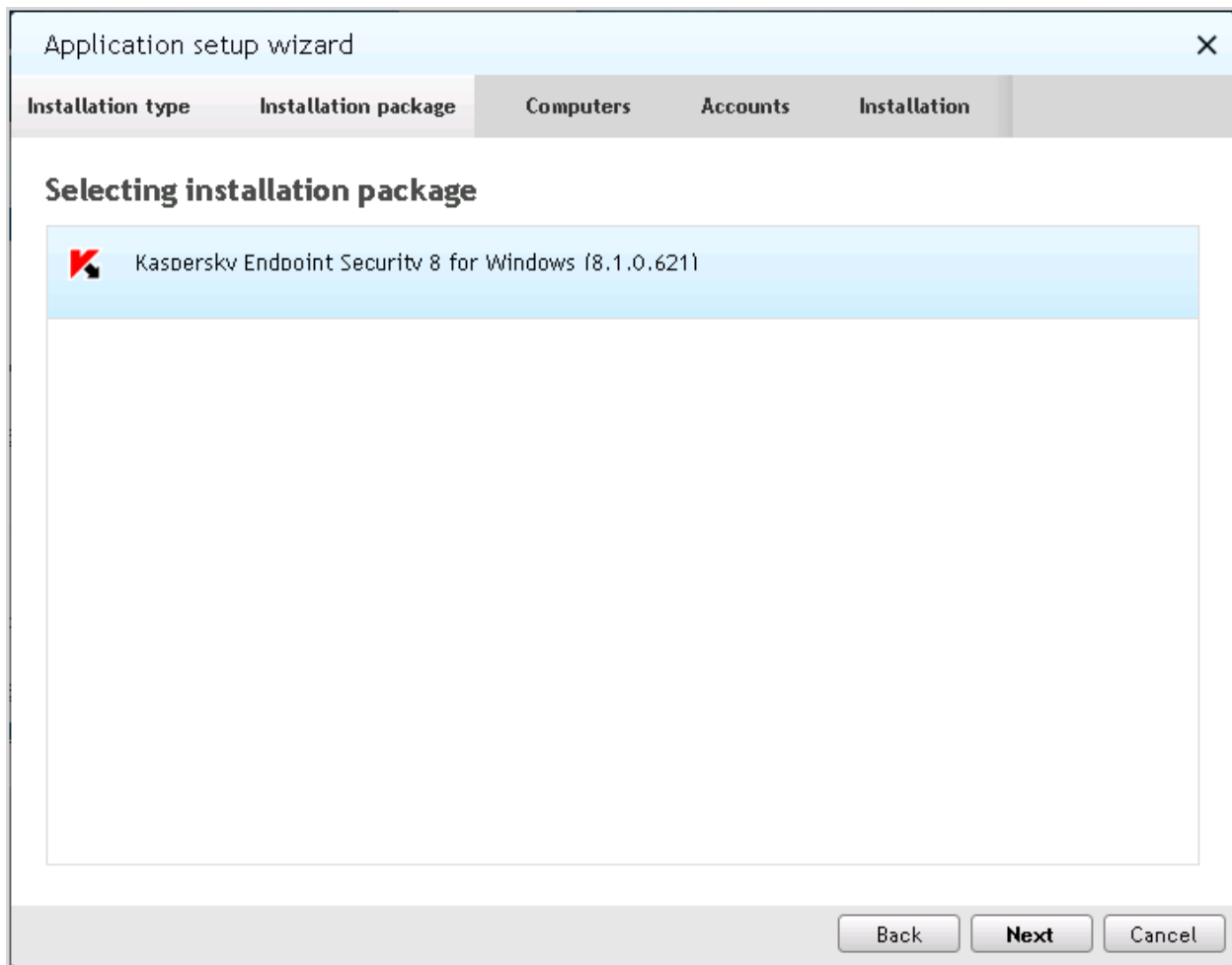


Figure 14. Application Setup Wizard. Selecting an installation package

5. In the list, click the application that you want to install, and then click the **Next** button.

A window opens that contains a list of the computers in your network on which you can install an anti-virus application (see the following figure).

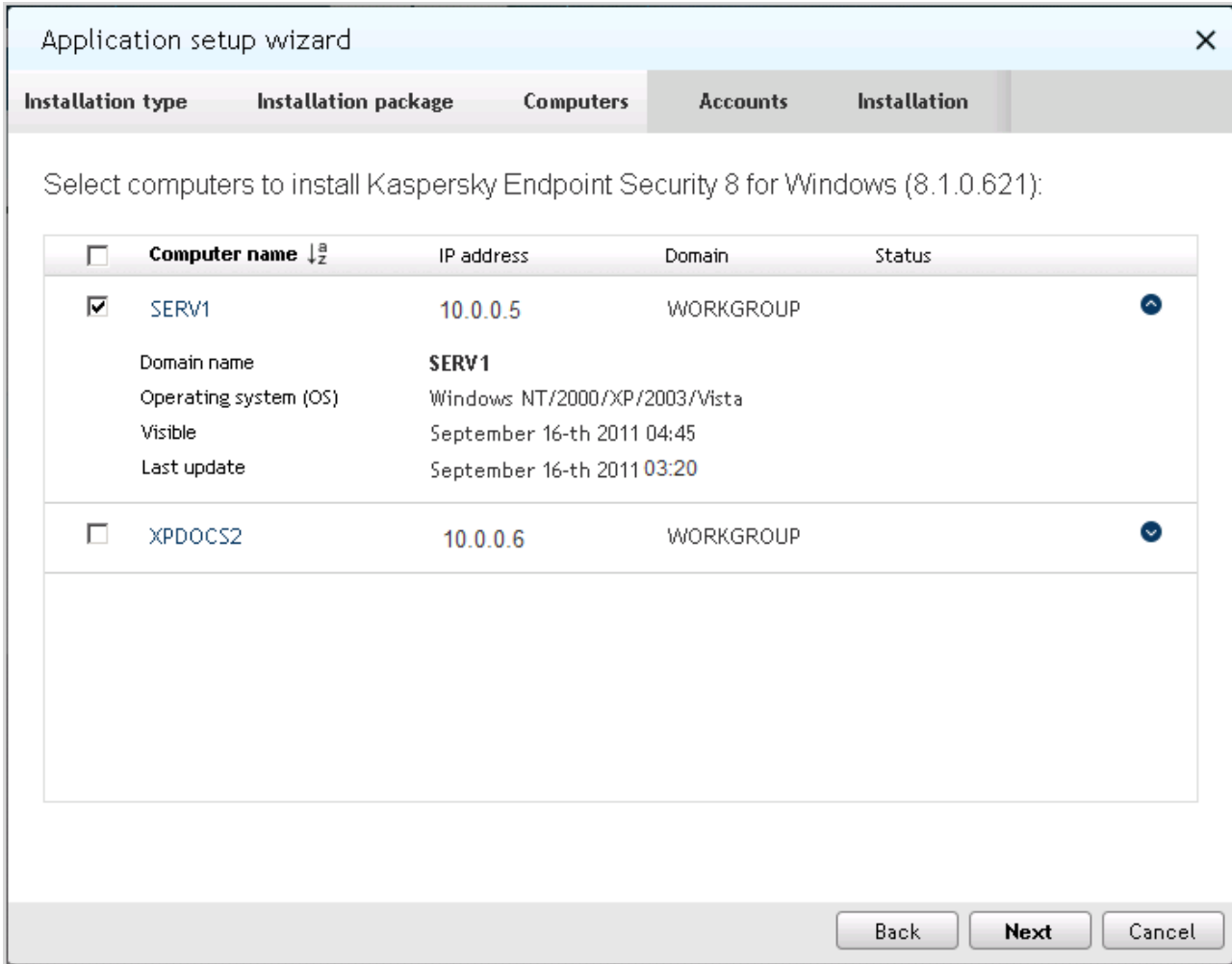


Figure 15. Application Setup Wizard. Selecting computers

If no computers are assigned an Update Agent status or have no Kaspersky Anti-Virus installed, the computers in your network are not displayed in the list of computers in the application setup wizard. In this case you cannot start a remote installation to the computers of your network.

6. Select the check boxes for the computers on which you want to install the application. If you want to install an anti-virus application on all computers in the list, select the **Computer name** check box. Click the **Next** button.

The **Adding accounts** window opens (see the following figure).

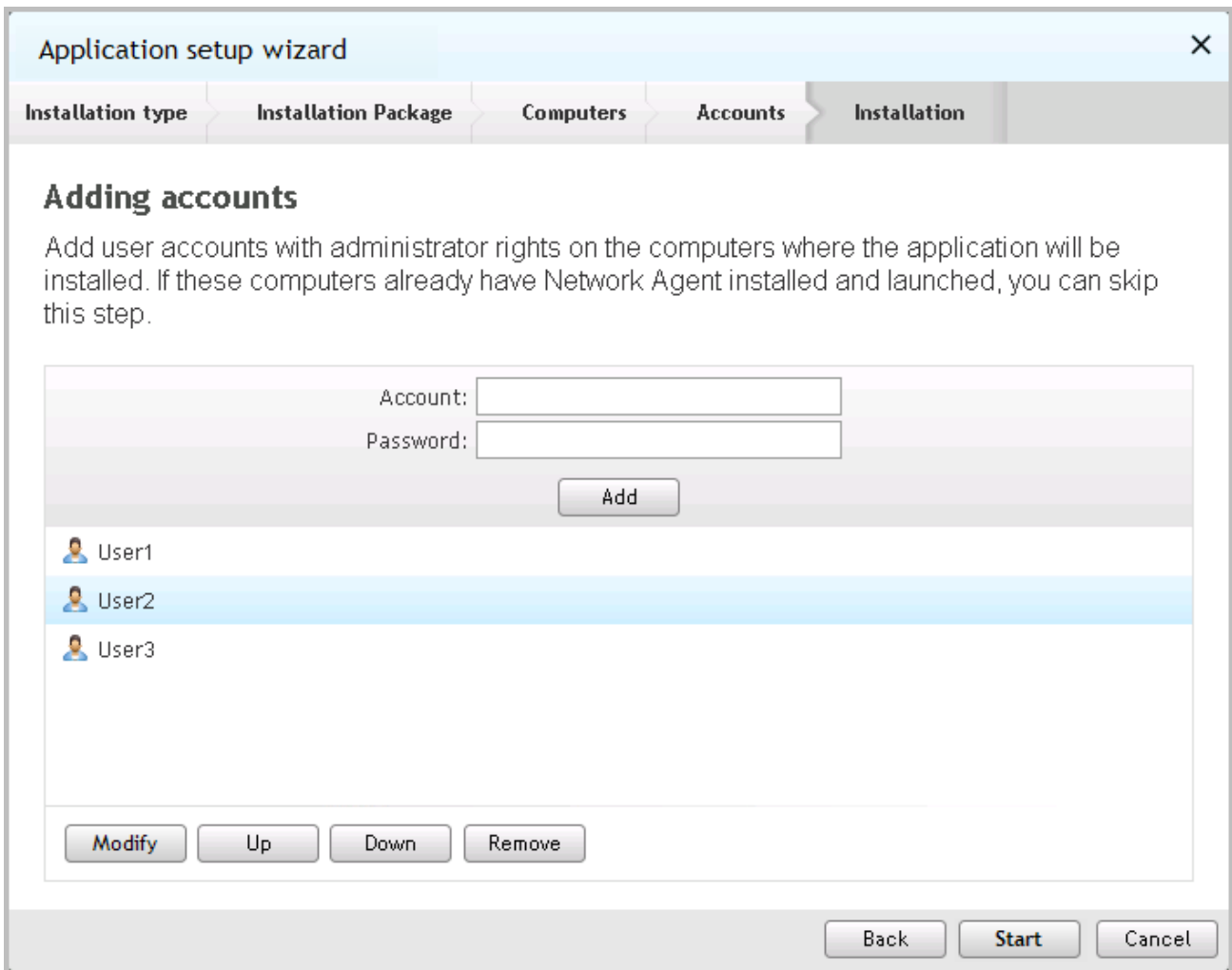


Figure 16. Application Setup Wizard. Adding accounts

- Create a list of accounts that have administrator privileges on computers that are selected for installation (see the following figure).
- To add accounts, for each account do the following:
  - a. In the **Account** text box, enter the account name.
  - b. In the **Password** text box, enter the password for the account.
  - c. Click the **Add** button.

The added account appears in a list in the lower part of the window.

- To modify settings of an account:
  - a. In the list select an account and click the **Modify** button.
  - b. Edit the account name in the **Account** text box.
  - c. Change the account password in the **Password** text box.

- d. Click the **Save changes** button (see the following figure).

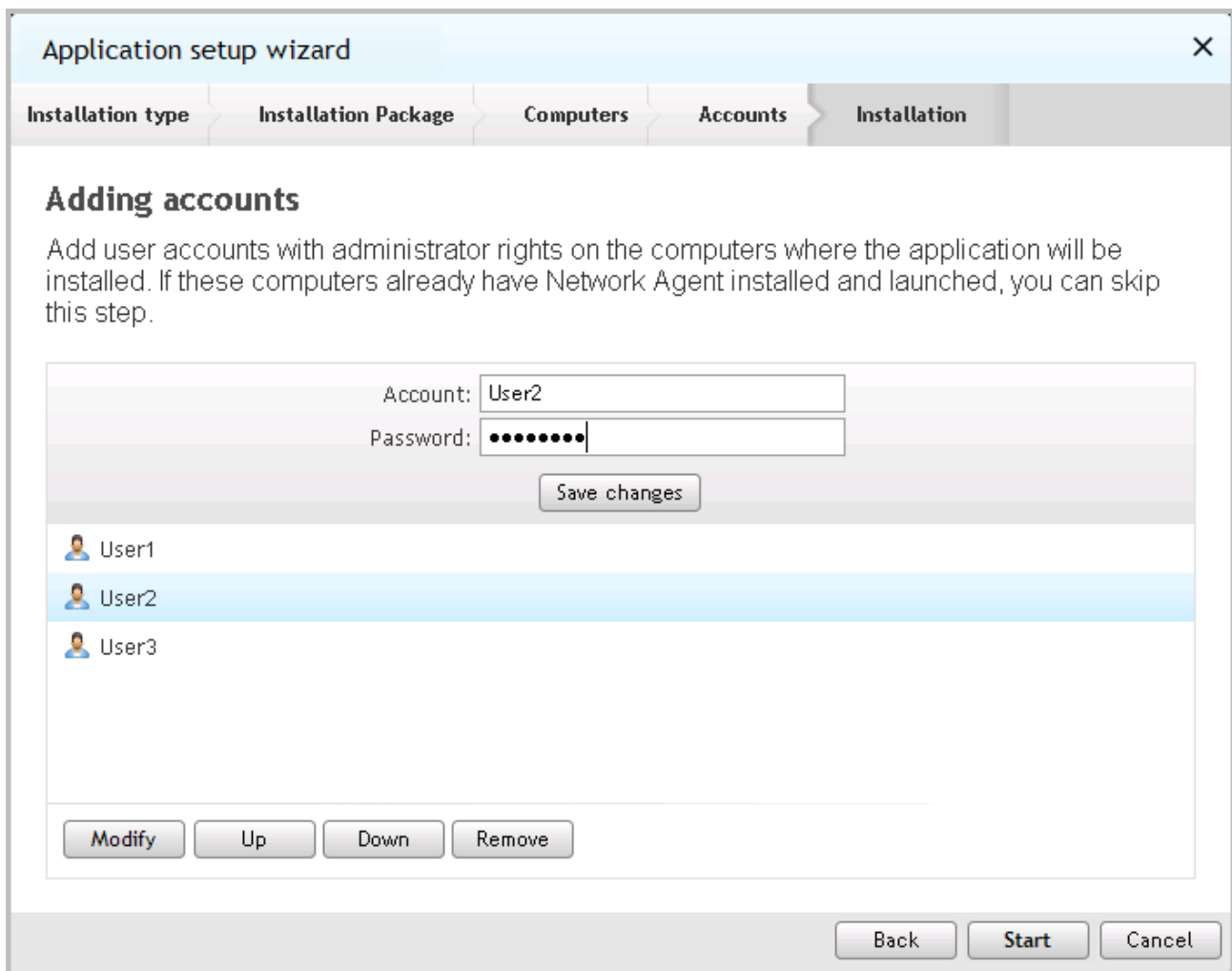


Figure 17. Application Setup Wizard. Modifying an account

The account's name and password will change.

- To delete an account from the list, in the list of accounts select an account that you want to delete and click the **Remove** button.
  - To modify the order in which the setup wizard applies the accounts when starting remote installation on computers:
    - To move the account up in the list, select an account and click the **Move up** button.
    - To move the account down in the list, select an account and click the **Move down** button.
7. Start the remote installation of anti-virus application by clicking the **Start** button.

The remote installation starts on the computers you selected. A new Wizard window opens that says **Installing <Application name> to the following computers**. The window lists the network computers on which the anti-virus application is being installed (see the following figure).

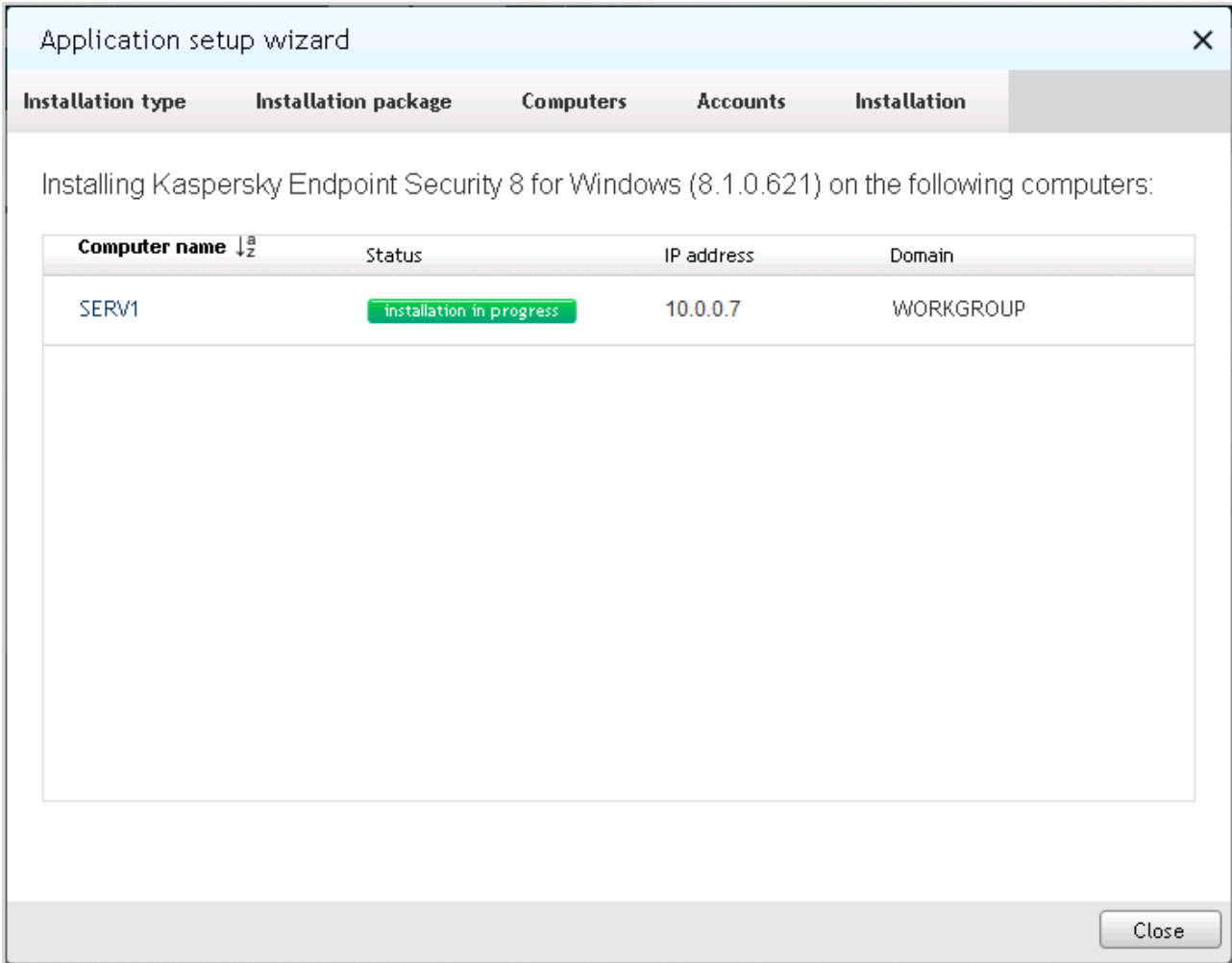


Figure 18. Application Setup Wizard. List of installations is progress

To view installation list, use the following interface elements:

Icon —Filters the installation list by the selected field in ascending or descending alphabetical order.

Icon —Opens the section of information about the selected computer.

Icon —Closes the section of computer information.

For each computer on which the remote installation of anti-virus application has been started, the installation list contains the following information:

- **Computer name.** Name in which a computer is registered in the network.
- **Status.** Status of the anti-virus application installation. After remote installation is started, the status changes to *Installation in progress*.
- **IP address.** Network address of the computer.
- **Domain.** Name of the network domain where the computer is registered.

8. To finish the setup wizard, click the **Close window** button. The installation tasks continue to run.

If a remote installation is successful, the computer is added automatically to the **Managed computers** administration group.

Remote installation of anti-virus applications is not always successful: for example, if another anti-virus application is already installed on a computer. Installations that complete with an error have the *Installation error* status. If remote installation of an anti-virus application completes with an error on one or more computers, you can install the application in the local installation mode.

You can start only one remote installation task. If you start a remote installation task before another installation task is finished, the first-started task will be interrupted.

## SEE ALSO:

About Update Agent.....	<a href="#">28</a>
About installing anti-virus applications .....	<a href="#">28</a>
Installing an anti-virus application manually .....	<a href="#">46</a>
Installing anti-virus applications to computer acting as Update Agent.....	<a href="#">30</a>

## VIEWING INFORMATION ABOUT THE STATUS OF AN ANTI-VIRUS REMOTE INSTALLATION

During remote installation of an anti-virus application you can view information about the installation status for each computer on which remote installation has been started.

➤ *To view status information about remote installation of an anti-virus application:*

1. Open the main application window (see section "Application interface" on page [11](#)).
2. Click the **Computers** tab.

- In the pane on the left click **Installation list**. The **List of active installations** window opens. The **List of active installations** window contains installations of anti-virus applications on in your network, and the status of those installations (see the following figure).

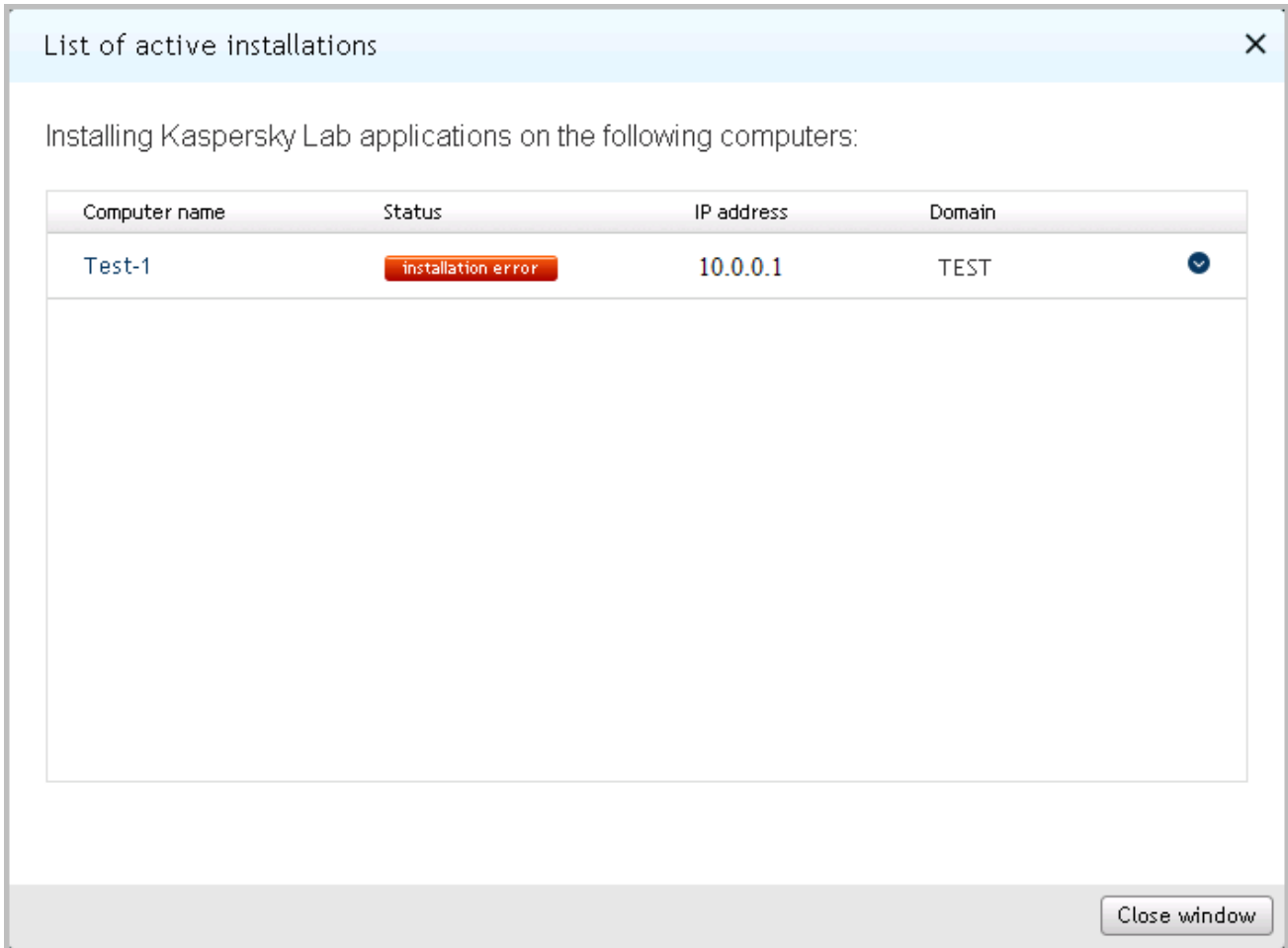


Figure 19. Status of the anti-virus application remote installation

The computers from the installation list can have the following statuses:

- Installation in progress*—Remote installation of the anti-virus application is not complete.
- Installation error*—Remote installation of the anti-virus application is complete with error. We recommend that you install the application manually.

**SEE ALSO:**

---

Installing anti-virus application remotely.....	<a href="#">33</a>
Installing an anti-virus application manually .....	<a href="#">46</a>

## LOCAL INSTALLATION MODE

You can install anti-virus applications to the computers of your network in remote installation mode. There are two ways to perform local installation:

- **Install manually using a distribution package.** You can download the distribution package to computer and *install anti-virus application manually*, following the setup wizard instructions. Manual installation (also referred to as "manual installation mode") requires your immediate participation in installing an anti-virus application on each computer. You can allow users of your network to install anti-virus applications manually on their computers. To do this, place the distribution packages to network shared folder.
- **Install by using published installation package.** To install an anti-virus application in this mode, publish the installation package of anti-virus application. After the publication is complete, Kaspersky Security Center Web-Console gives you a link to the published installation package. By using this link you can download the published installation package to computer and run it. After you run a published installation package, an anti-virus application is installed automatically. You can allow users of your network to install anti-virus applications independently on their computers using published installation packages. To do this, you should only send them links to published installation packages.

### IN THIS SECTION

---

Publishing installation packages .....	<a href="#">41</a>
Viewing a list of published installation packages .....	<a href="#">43</a>
Cancelling publication of installation package .....	<a href="#">44</a>
Installing anti-virus application by using published installation package .....	<a href="#">45</a>
Installing an anti-virus application manually .....	<a href="#">46</a>

## PUBLISHING INSTALLATION PACKAGES

➡ *To publish installation packages:*

1. Open the main application window (see section "Application interface" on page [11](#)).
2. Click the **Computers** tab.
3. Click the **Add package** link in the left part of the window to open the **Adding packages** window.

A window will open that contains all installation packages that you can publish (see the figure below).

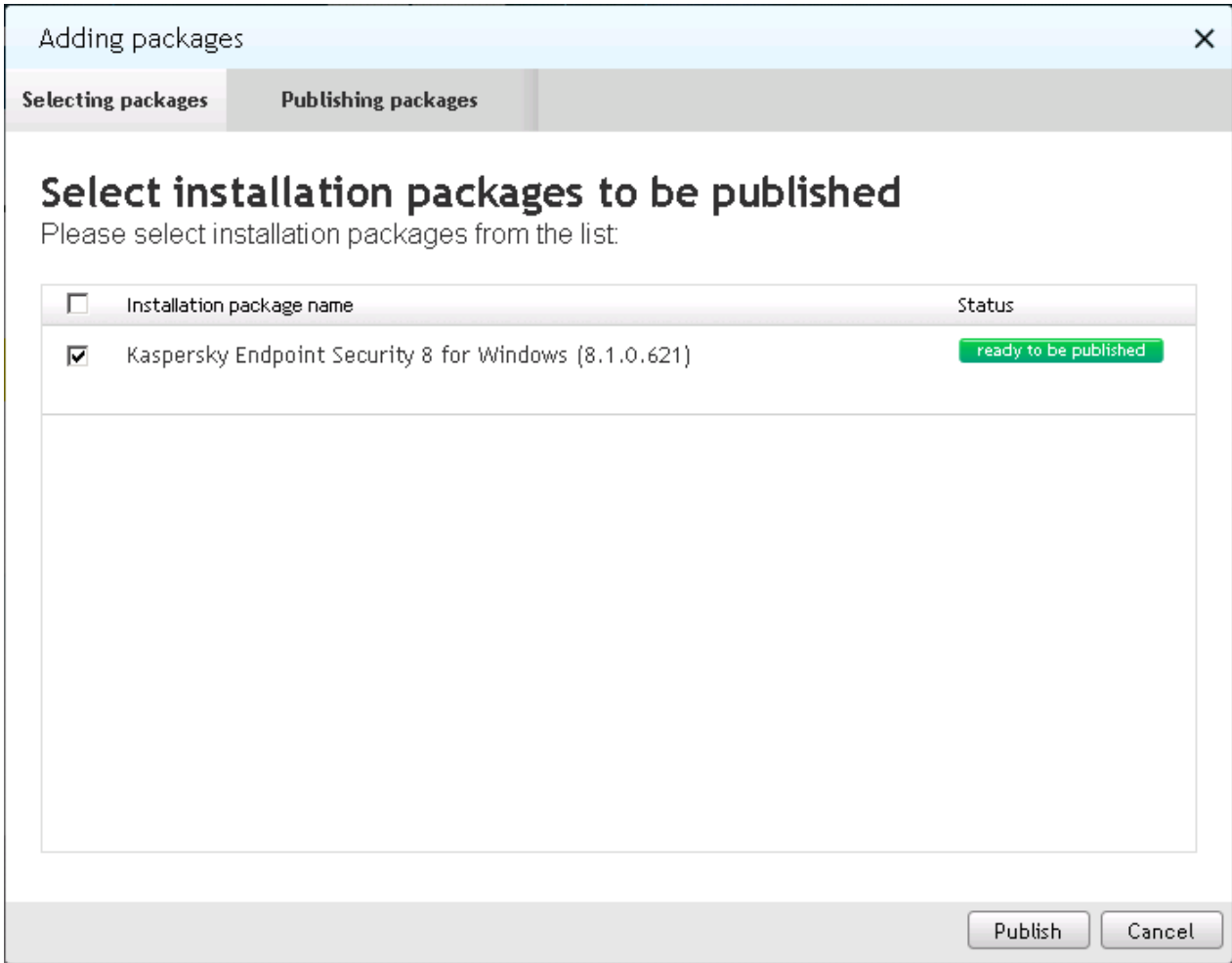


Figure 20. Publishing packages

4. Select the check boxes for the installation packages that you want to publish. If you want to publish all installation packages from the list, select the check box next to the heading **Installation package name**.
5. Click the **Publish** button.

The status of selected installation packages will change to *publishing*. The publication of selected packages will start.

6. Click the **Close** button to close the **Adding packages** window.

The installation packages will be published automatically. After the publication is finished, installation packages are added to the published installation packages list.

**SEE ALSO:**

---

About how to publish installation packages.....	<a href="#">29</a>
Cancelling publication of installation package.....	<a href="#">44</a>
Viewing a list of published installation packages.....	<a href="#">43</a>

## VIEWING A LIST OF PUBLISHED INSTALLATION PACKAGES

➤ To view a list of published installation packages:

1. Open the main application window (see section "Application interface" on page [11](#)).
2. Click the **Computers** tab.
3. Click the **Packages list** link in the left part of the window to open the **List of installation packages** window.

This opens the window containing published installation packages (see the figure below).

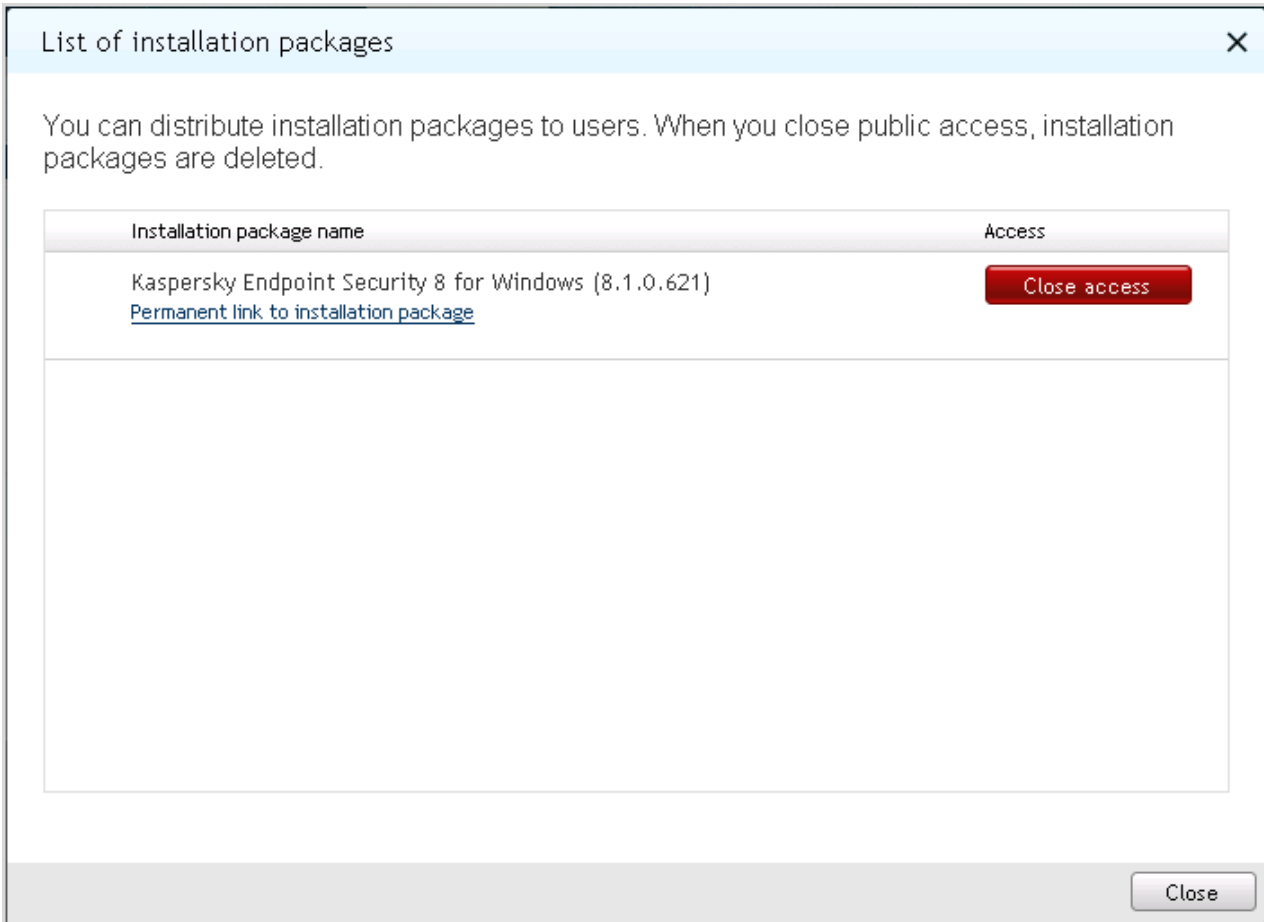


Figure 21. List of published installation packages

The list contains the following information about installation packages:

- **Installation package name.** Name of published installation package.
- **Permanent link to installation package.** Link that you can use to download the installation package from local network.

If later version of installation package is available on Administration Server, you can update the package by using the **Update** button, located next to the installation package.

You can send links to published installation packages to the users of your network (for example, by email). The users of your network can use them to download published installation packages to their computers and to install anti-virus applications.

SEE ALSO:

About how to publish installation packages..... 29

## CANCELLING PUBLICATION OF INSTALLATION PACKAGE

You may need to cancel the upload of installation package for example, if it's outdated.

➔ To cancel the publication of installation package:

1. Open the main application window (see section "Application interface" on page 11).
2. Click the **Computers** tab.
3. Click the **Packages list** link in the left part of the window to open the **List of installation packages** window.

This opens the window containing published installation packages (see the figure below).

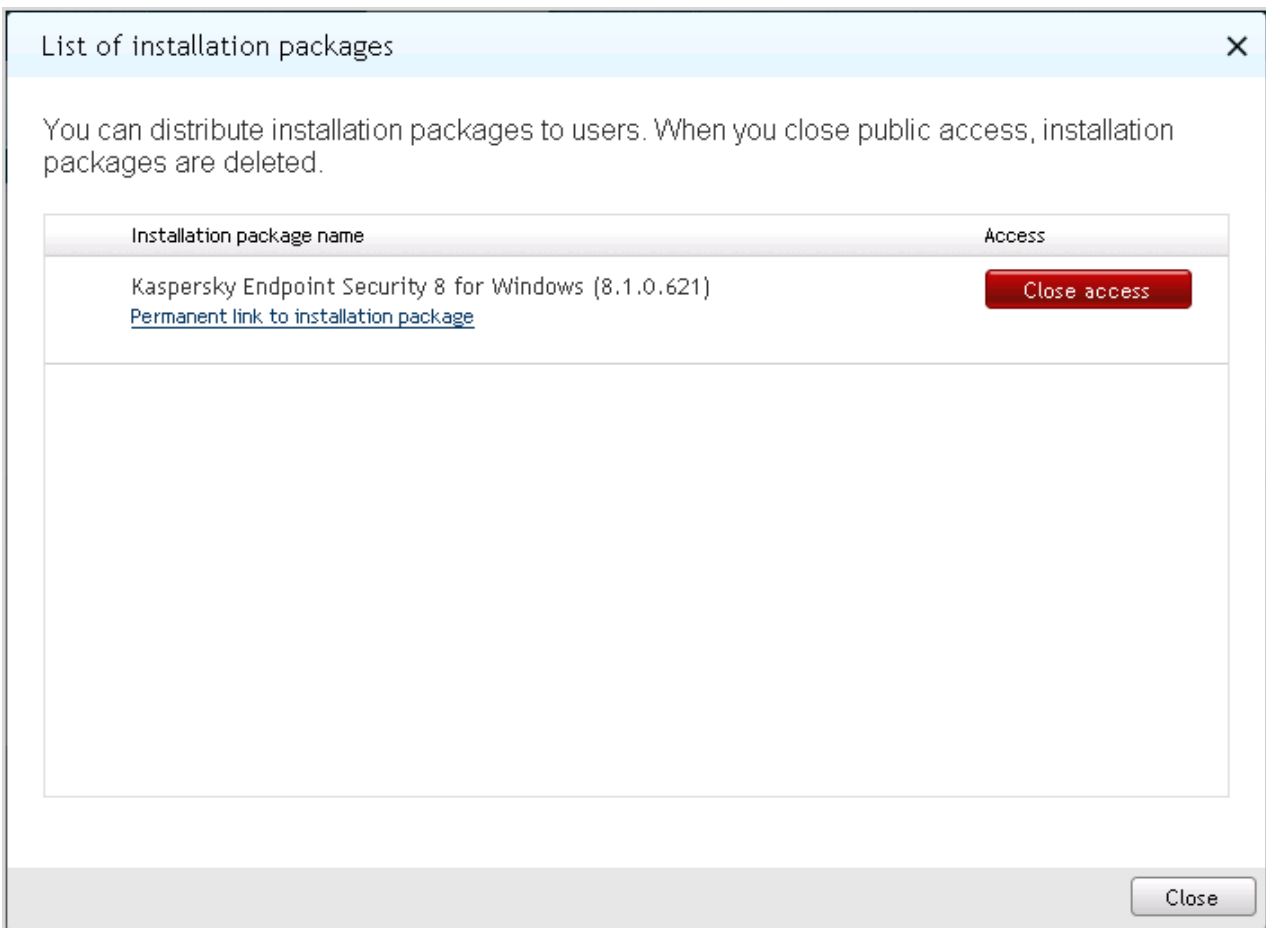


Figure 22. List of published installation packages

4. Find an installation package for which you want to cancel the publication and click the **Close access** button next to it.

The string will display a message: *package removed, access is closed* (see the figure below). Publication of installation package will be cancelled. The package becomes unavailable.

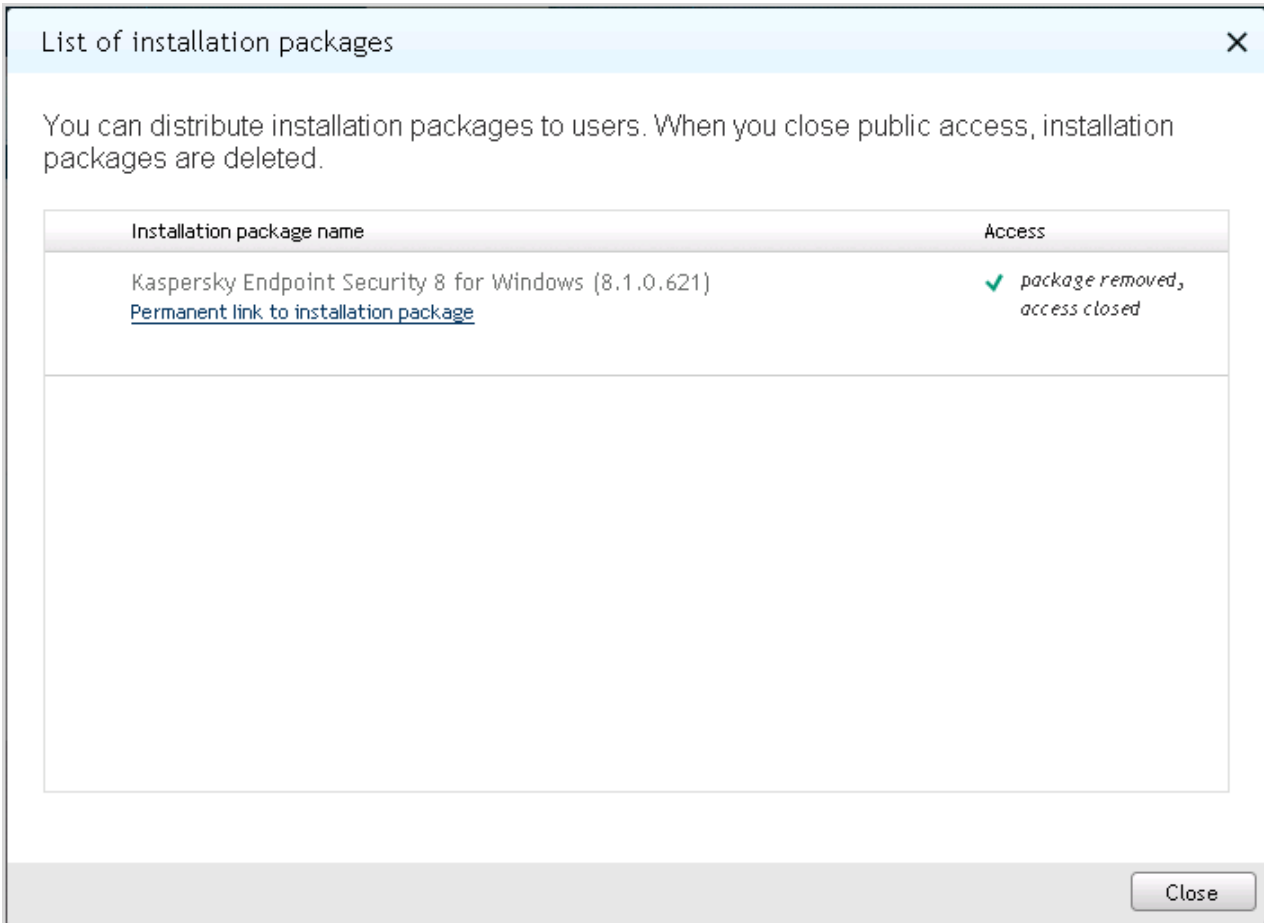


Figure 23. Cancelling package publication

- To close the **List of installation packages** window, click the **Close** button.

**SEE ALSO:**

About how to publish installation packages..... [29](#)

**INSTALLING ANTI-VIRUS APPLICATION BY USING PUBLISHED INSTALLATION PACKAGE**

➔ *To install an anti-virus application by using a published installation package:*

- Download the published installation package to a computer where you want the anti-virus application installed. To do this, use the link received after the package is finished.
- Run published installation package. The installation is performed automatically.
- Wait until the installation is finished.

## INSTALLING AN ANTI-VIRUS APPLICATION MANUALLY

➤ To install an anti-virus application manually:

1. Open the main application window (see section "Application interface" on page [11](#)).
2. Click the **Computers** tab.
3. Click the **Add computer** link in the pane to the left to start the Application Setup Wizard.

The Application Setup Wizard opens with a Welcome page (see the following figure).

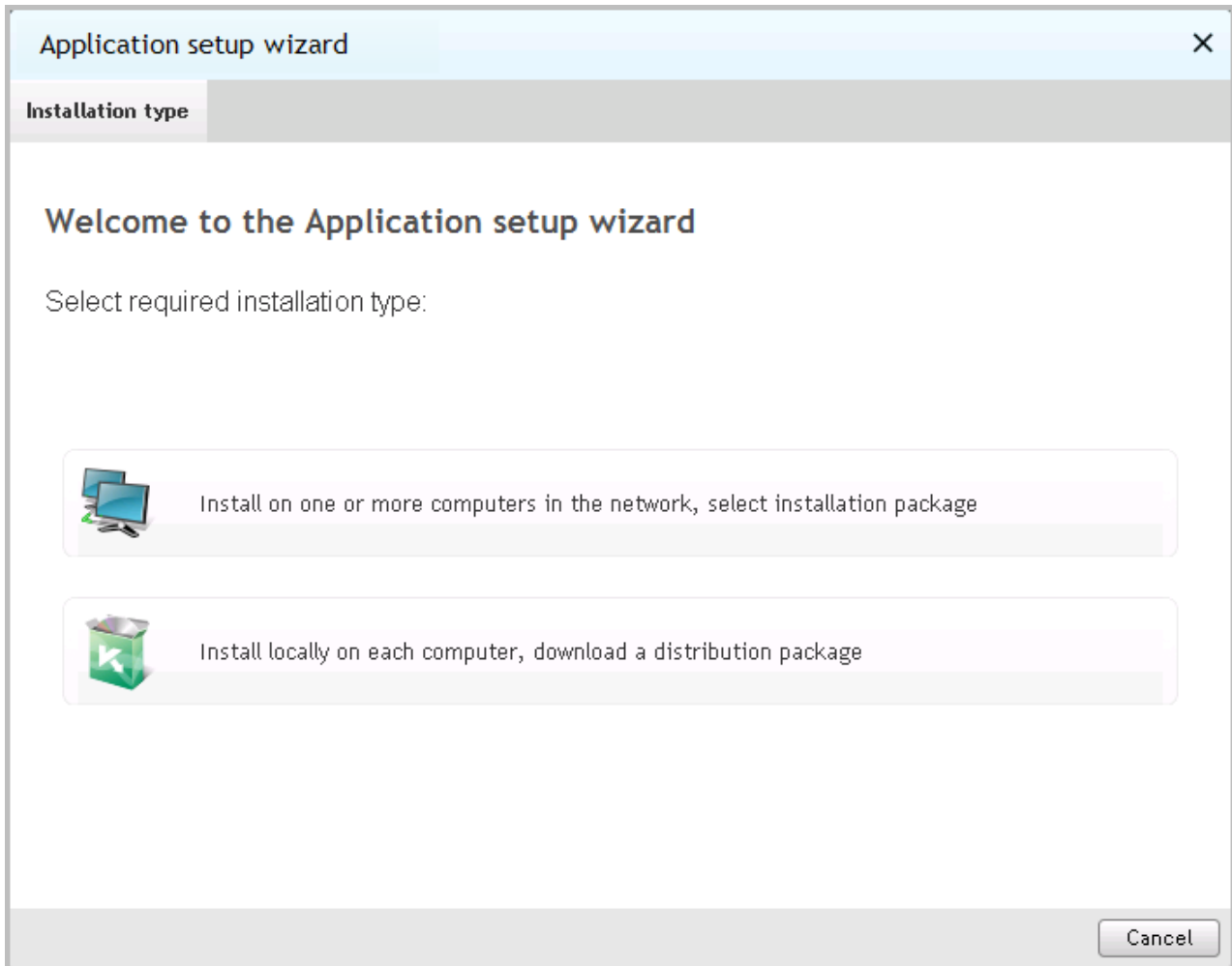


Figure 24. Application Setup Wizard. Welcome page

4. Click the button **Install locally on each computer, download a distribution package**.

The **Select a distribution package to download** window opens (see the figure below).

If no published installation packages are discovered, you will be asked to publish installation packages (see section "Publishing installation packages" on page 41). After installation packages are published, the installation of anti-virus application will continue.

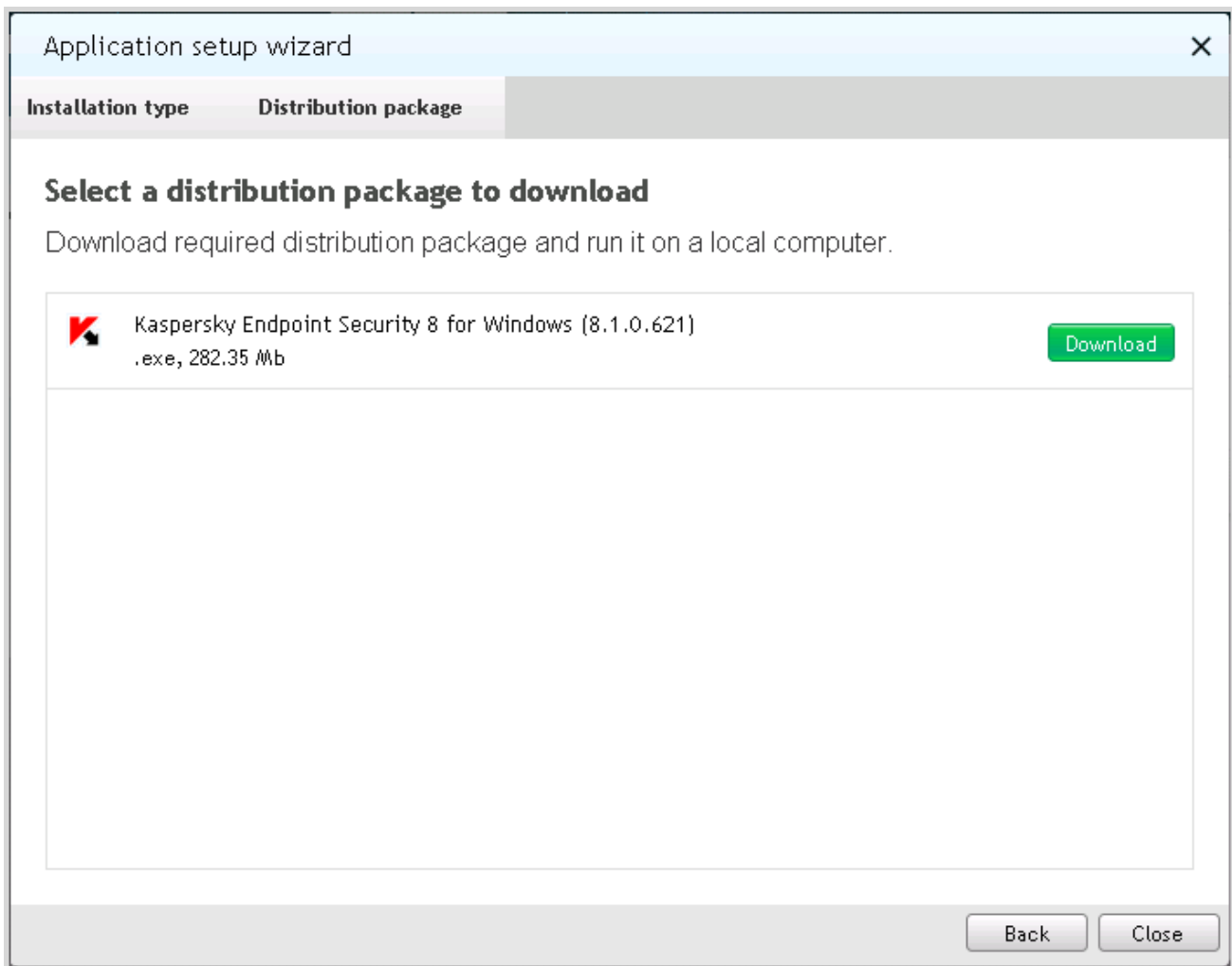


Figure 25. Application Setup Wizard. Downloading an installation package

5. Select the installation package that you want to install manually and click the **Download** button next to the application name.
6. Click the **Finish** button. The Application Setup Wizard closes.
7. Run the installation package on each computers where you want the anti-virus application installed. Then follow the instructions of the installation package wizard.

The computers on which the anti-virus application is successfully installed are automatically added to the **Managed computers** administration group.

These computers are displayed in the computer list the next time you log on to Kaspersky Security Center Web-Console portal or update the list.

If during installation an error message is displayed, contact your service provider's administrator.

**SEE ALSO:**

---

About installing anti-virus applications ..... [28](#)

Viewing a list of computers..... [23](#)

Connecting to Administration Server ..... [13](#)

Installing anti-virus applications to computer acting as Update Agent..... [30](#)

# WORKING WITH REPORTS

This section describes how to perform the following operations on reports provided by the Administration Server to which the application is connected: view, print, send by email, and save report data to file.

## IN THIS SECTION

---

About reports.....	<a href="#">49</a>
Actions on reports .....	<a href="#">49</a>
Viewing reports .....	<a href="#">50</a>
Exporting reports.....	<a href="#">51</a>
Configuring report delivery .....	<a href="#">51</a>

## ABOUT REPORTS

Kaspersky Security Center Web-Console allows you with to gain access to reports of the Administration Server to which the application is connected.

Reports include data about the status of anti-virus protection on computers managed by Administration Server. Such information includes data on installed applications, licenses, viruses, ant-virus databases, infected computers, and errors.

The list of available reports is created by your service provider's administrator. The list of reports can vary depending on the access rights assigned to your account.

## ACTIONS ON REPORTS

You can perform the following operations on Administration Server reports:

- **View reports**

You can view reports published for you by the service provider's administrator. The reports are read-only. You cannot modify them.

- **Export reports**

After viewing a report, you can export it and save it, for example, for later analysis and processing. You can export a report to one of three formats: HTML, XML, or PDF.

- **Configure automatic report delivery by email**

Administration Server permits automatic delivery of reports by email. You might have to configure Kaspersky Security Center Web-Console to deliver reports by email to you and other staff members involved in network anti-virus protection; for example, system administrators or other IT specialists.

You can manage automatic report delivery by modifying the delivery settings: set of delivered reports and list of recipients' email addresses. All recipients in the list receive the same set of reports.

Administration Server sends reports once a day, at midnight.

**SEE ALSO:**

Viewing reports ..... 50

Exporting reports ..... 51

Configuring report delivery ..... 51

## VIEWING REPORTS

➔ To view a report:

1. Open the main application window (see section "Application interface" on page 11).
2. Click the **Reports** tab.
3. In the left part of the window, from the list of reports, select a report you want to view (see the following figure).

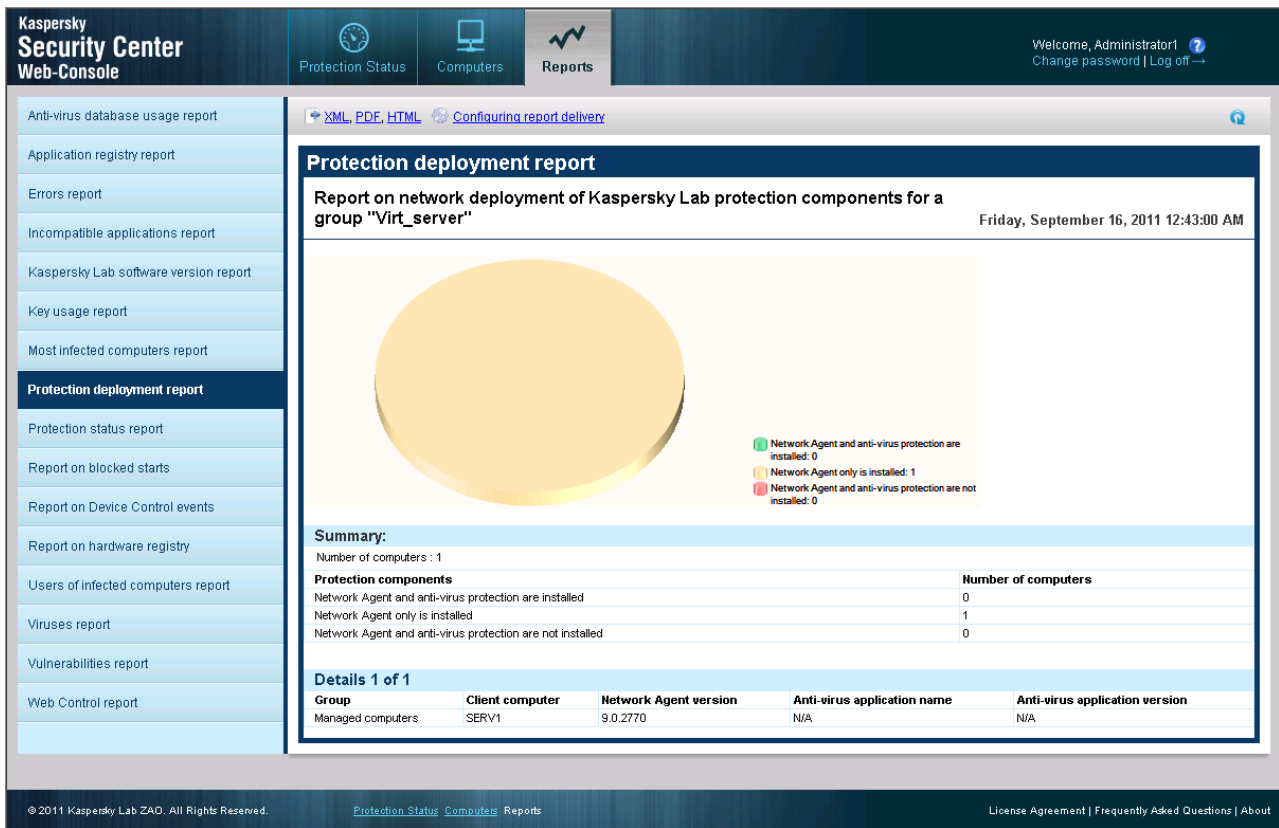


Figure 26. Viewing reports

In the right part of the window, the report contents are displayed. In the upper-right part of the window, the date and time of the report creation are displayed.

You can update the report contents to view updated data.

➔ To update report contents:

Click the  button in the upper-right corner of the window.

## EXPORTING REPORTS

➔ *To export a report:*

1. Open the main application window (see section "Application interface" on page [11](#)).
2. Click the **Reports** tab.
3. In the left part of the window, click a report that you want to export.

In the right part of the window, the report contents are displayed.

4. In the upper part of the window, click the link for the export format you want:
  - To export a report in XML format, click **XML**.
  - To export a report in PDF format, click **PDF**.
  - To export a report in HTML format, click the **HTML**.

The report in the selected format opens in the web browser window or in the window of a viewing application associated with the selected format (such as Acrobat Reader, for .pdf).

5. Save the report to file by using browser tools or the viewing application.

## CONFIGURING REPORT DELIVERY

➔ *To configure report delivery by email:*

1. Open the main application window (see section "Application interface" on page [11](#)).
2. Click the **Reports** tab.
3. Click the link in the upper part of the main window (see the figure below). The **Configuring reports delivery** window opens.

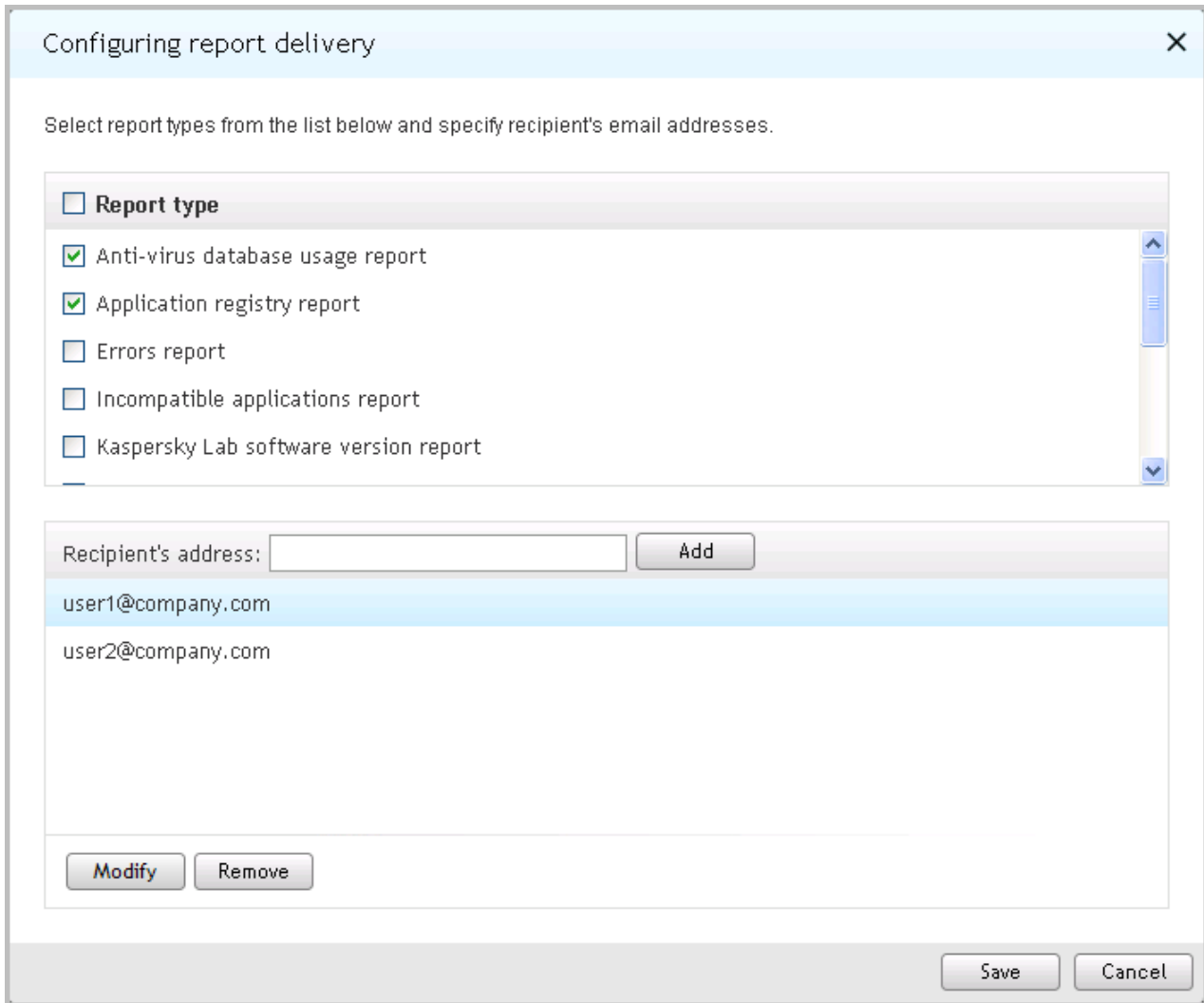


Figure 27. Configuring report delivery

4. In the list of reports, select the check boxes next to reports that you want to include in the delivery. If you want to include all reports in the delivery, select the check box next to **Report type**.
5. Create a delivery list containing recipient email addresses:
  - To add an email address to the delivery list:
    - a. Enter the email address in the **Recipient's address** text box.
    - b. Click the **Add** button.

The new email address is displayed in the delivery list.
  - To remove an email address from the delivery list, select an address that you want to remove and click the **Remove** button.
  - To modify an email address in the delivery list:
    - a. In the delivery list, click an email address that you want to modify and click the **Modify** button.

The selected email address is removed from the delivery list and is displayed in the **Recipient's address** text box.

- b. Change the email address in the **Recipient's address** text box, and click the **Add** button.

The new email address is displayed in the delivery list.

6. Click the **Save** button.

The notification delivery settings are applied immediately.

# CHANGING YOUR ACCOUNT PASSWORD

You can change the password of your account after you log on to Kaspersky Security Center Web-Console. You might have to change your password, for example, if you want to set a password that is easier to remember.

➤ *To change the password of your account:*

1. Open the main application window (see section "Application interface" on page [11](#)).
2. In the upper-right corner of the screen, click the **Change password** link. The **Change password** window opens (see the following figure).

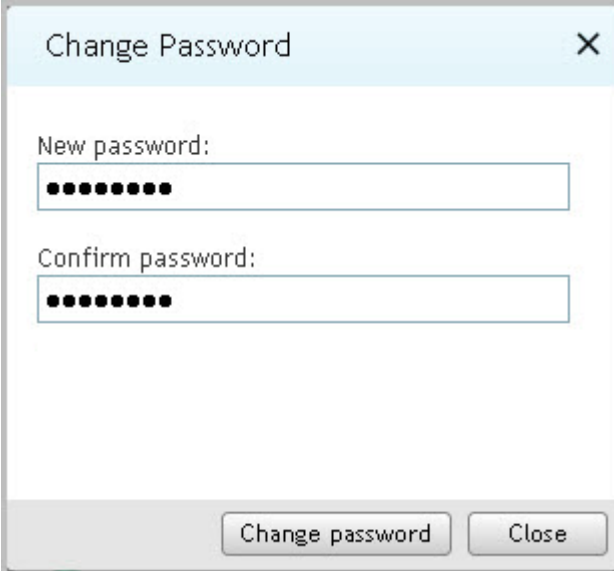


Figure 28. Changing your password

3. In the **New password** and **Confirm password** text boxes enter the new password.
4. Click the **Change password** button.

The password of your account is changed.

# LOGGING OFF KASPERSKY SECURITY CENTER WEB-CONSOLE

You can log off Kaspersky Security Center Web-Console from any tab on the application interface.

Before you exit the application, log off Kaspersky Security Center Web-Console.

If you exit the web browser without logging off (for example, by closing the browser's window or a tab), your session remains active for 24 hours.

➤ *To log off Kaspersky Security Center Web-Console:*

from the main application window (see section "Application interface" on page [11](#)), click the **Log off** link in the top right corner of the application.

You will log off Kaspersky Security Center Web-Console. In the web browser an entry window for user name and password will open (see section "Connecting to Administration Server" on page [13](#)).

# GLOSSARY

## A

### **ADMINISTRATION GROUP**

A set of computers grouped by function and installed Kaspersky Lab applications. Computers are grouped as a single entity for the convenience of management. An administration group can contain other administration groups. For each application installed in an administration group, group policies and tasks can be created.

### **ADMINISTRATION SERVER**

A component of Kaspersky Security Center that centralizes the storage of information about Kaspersky Lab applications installed on the corporate network and about the management of those applications.

### **ANTI-VIRUS PROTECTION SERVICE PROVIDER**

An organization that provides anti-virus protection services based on Kaspersky Lab solutions.

## C

### **CLIENT ADMINISTRATOR**

A staff member of a client company who is responsible for the anti-virus protection status.

## H

### **HTTPS**

Secure protocol for data transfer, using encryption, between a web browser and a web server. HTTPS is used to gain access to restricted information, such as corporate or financial data.

## I

### **INSTALLATION PACKAGE**

A set of files created for remote installation of a Kaspersky Lab application by using the Kaspersky Security Center Web-Console remote administration system. An installation package is created on the basis of special files with .kpd and .kud extensions that are included in the application distribution package; the installation package contains a set of settings that are required for application setup and post-installation configuration. By default, setting values match the application setting values.

## J

### **JAVASCRIPT**

A programming language that expands the performance of web pages. Web pages created using JavaScript can perform functions (for example, change the view of interface elements or open additional windows) without refreshing the web page with new data from a web server. To view pages created by using JavaScript, enable the JavaScript support in the configuration of your web browser.

## L

### **LOCAL INSTALLATION**

Installation of anti-virus application to a computer that belongs to corporate network. Such installation implies that you first download an installation package to this computer, then run a published installation package, or start the installation manually from the anti-virus distribution package.

## M

### **MANAGED COMPUTERS**

Corporate network computers that are included in an administration group.

**MANUAL INSTALLATION**

Installation of an anti-virus application to a network computer by means of an anti-virus application distribution package. Manual installation does not require direct participation by a system administrator or other IT specialist. Usually manual installation is done if remote installation has completed with an error.

**N****NETWORK ANTI-VIRUS PROTECTION**

A set of technical and organizational measures that lower the probability that viruses and spam will penetrate an enterprise network, and that block network attacks, phishing, and other threats. Network security increases when anti-virus applications and services are used and when a corporate information security policy is in place.

**NETWORK PROTECTION STATUS**

The current protection status, which defines the safety of corporate network computers. The network protection status includes such factors as installed anti-virus applications, active and additional keys, quantity and types of detected threats.

**R****REMOTE INSTALLATION**

Installation of Kaspersky Lab applications using the services provided by Kaspersky Security Center Web-Console.

**S****SERVICE PROVIDER'S ADMINISTRATOR**

A staff member at an anti-virus protection service provider. This administrator performs installation and maintenance jobs for anti-virus protection systems based on Kaspersky Lab anti-virus products and also provides technical support to customers.

**SSL**

A data encryption protocol on the Internet and local networks. SSL is used in web applications to create secure connection between a client and a server.

**U****UPDATE AGENT**

Computer acting as an intermediate source for distribution of updates and installation packages in an administration group.

**W****WEB PORTAL**

A means of access over a web browser to the features of Kaspersky Security Center Web-Console. A web portal consists of web pages that contain text and graphical information and management add-ins for Kaspersky Security Center Web-Console. Web pages open in the web browser after you log on to the web portal. To log on to a web portal, you must have the web portal address, account name and password.

# KASPERSKY LAB ZAO

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

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

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

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

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

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

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

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

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

Kaspersky Lab's website:

<http://www.kaspersky.com>

Virus encyclopedia:

<http://www.securelist.com>

Anti-virus laboratory:

[newvirus@kaspersky.com](mailto:newvirus@kaspersky.com)

(only for sending probably infected files in archive format)

<http://support.kaspersky.ru/virlab/helpdesk.html?LANG=en>

(for queries addressed to virus analysts)

Kaspersky Lab's web forum:

<http://forum.kaspersky.com>

# INFORMATION ABOUT THIRD-PARTY CODE

Third-party code was used during the application development.

## IN THIS SECTION

---

C++ JSON PARSER 4.03 .....	<a href="#">59</a>
FCGI-2.4.1-SNAP-0910052249 .....	<a href="#">59</a>
ICU 4.4 (INTERNATIONAL COMPONENTS FOR UNICODE) .....	<a href="#">60</a>
MOD_FCGI-SNAP-0910052141 .....	<a href="#">60</a>

## C++ JSON PARSER 4.03

C++ JSON Parser 4.03

Copyright (C) 2007 – 2009, John W. Wilkinson

-----

The MIT License

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## FCGI-2.4.1-SNAP-0910052249

fcgi-2.4.1-SNAP-0910052249

Copyright (C) 1996, Open Market, Inc.

-----

This FastCGI application library source and object code (the "Software") and its documentation (the "Documentation") are copyrighted by Open Market, Inc ("Open Market"). The following terms apply to all files associated with the Software and Documentation unless explicitly disclaimed in individual files.

Open Market permits you to use, copy, modify, distribute, and license this Software and the Documentation for any purpose, provided that existing copyright notices are retained in all copies and that this notice is included verbatim in any distributions. No written agreement, license, or royalty fee is required for any of the authorized uses. Modifications to this

Software and Documentation may be copyrighted by their authors and need not follow the licensing terms described here. If modifications to this Software and Documentation have new licensing terms, the new terms must be clearly indicated on the first page of each file where they apply.

OPEN MARKET MAKES NO EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE SOFTWARE OR THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL OPEN MARKET BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY DAMAGES ARISING FROM OR RELATING TO THIS SOFTWARE OR THE DOCUMENTATION, INCLUDING, WITHOUT LIMITATION, ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES OR SIMILAR DAMAGES, INCLUDING LOST PROFITS OR LOST DATA, EVEN IF OPEN MARKET HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOFTWARE AND DOCUMENTATION ARE PROVIDED "AS IS". OPEN MARKET HAS NO LIABILITY IN CONTRACT, TORT, NEGLIGENCE OR OTHERWISE ARISING OUT OF THIS SOFTWARE OR THE DOCUMENTATION.

## ICU 4.4 (INTERNATIONAL COMPONENTS FOR UNICODE)

ICU 4.4 (International Components for Unicode)

Copyright (C) 1995-2010, International Business Machines Corporation and others

-----  
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

## MOD\_FCGI-SNAP-0910052141

mod\_fcgi-SNAP-0910052141

Copyright (C) 1995-1996, Open Market, Inc.

-----  
This FastCGI application library source and object code (the "Software") and its documentation (the "Documentation") are copyrighted by Open Market, Inc ("Open Market"). The following terms apply to all files associated with the Software and Documentation unless explicitly disclaimed in individual files.

Open Market permits you to use, copy, modify, distribute, and license this Software and the Documentation solely for the purpose of implementing the FastCGI specification defined by Open Market or derivative specifications publicly endorsed by Open Market and promulgated by an open standards organization and for no other purpose, provided that existing copyright notices are retained in all copies and that this notice is included verbatim in any distributions.

No written agreement, license, or royalty fee is required for any of the authorized uses. Modifications to this Software and Documentation may be copyrighted by their authors and need not follow the licensing terms described here, but the modified Software and Documentation must be used for the sole purpose of implementing the FastCGI specification defined by Open Market or derivative specifications publicly endorsed by Open Market and promulgated by an open standards organization and for no other purpose. If modifications to this Software and Documentation have new licensing terms, the new terms must protect Open Market's proprietary rights in the Software and Documentation to the same extent as these licensing terms and must be clearly indicated on the first page of each file where they apply.

Open Market shall retain all right, title and interest in and to the Software and Documentation, including without limitation all patent, copyright, trade secret and other proprietary rights.

OPEN MARKET MAKES NO EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE SOFTWARE OR THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL OPEN MARKET BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY DAMAGES ARISING FROM OR RELATING TO THIS SOFTWARE OR THE DOCUMENTATION, INCLUDING, WITHOUT LIMITATION, ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES OR SIMILAR DAMAGES, INCLUDING LOST PROFITS OR LOST DATA, EVEN IF OPEN MARKET HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOFTWARE AND DOCUMENTATION ARE PROVIDED "AS IS". OPEN MARKET HAS NO LIABILITY IN CONTRACT, TORT, NEGLIGENCE OR OTHERWISE ARISING OUT OF THIS SOFTWARE OR THE DOCUMENTATION.

# TRADEMARK NOTICES

Registered trademarks and service marks are the property of their respective owners.

Debian is a registered trademark of Software in the Public Interest, Inc.

Fedora and the Infinity design logo are trademarks of Red Hat, Inc.

Microsoft, Windows and Internet Explorer are registered trademarks of Microsoft Corporation in the United States and other countries.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Red Hat and Red Hat Enterprise Linux are registered trademarks of Red Hat, Inc. in the U.S. and other countries.

Mac OS, Safari, Leopard, Snow Leopard, Tiger are registered trademarks of Apple Inc.

Mozilla and Firefox are trademarks of the Mozilla Foundation.

# INDEX

## A

Account .....	13
name .....	13
password .....	13
settings .....	13
ACCOUNT	
PASSWORD.....	54
Administration groups.....	23, 56
ADMINISTRATION GROUPS .....	17
Administration Server.....	56
connection .....	13
ADMINISTRATION SERVER.....	8, 17
Anti-virus application .....	28
ANTI-VIRUS PROTECTION	
SERVICE PROVIDER .....	8
ANTI-VIRUS PROTECTION SERVICE PROVIDER .....	8
ANTI-VIRUS SECURITY.....	8
Automatic report delivery.....	49, 51

## C

CLIENT .....	8
Client administrator .....	5
CLIENT ADMINISTRATOR.....	8
Computer properties .....	25
COMPUTER STATUS.....	17
Computers	
IP address .....	25
list .....	23
managed.....	23, 25
name .....	25
properties.....	25
unassigned .....	23, 25
COMPUTERS .....	17
MANAGED .....	17
NAME .....	17
UNASSIGNED.....	17
Connection .....	13

## H

HTTPS .....	8
-------------	---

## I

INFORMATIONAL AREA .....	11
Installation	
manual.....	46
remote .....	33
wizard .....	33
Installation package .....	28

## J

JavaScript .....	13
------------------	----

**K**

KASPERSKY ANTI-VIRUS .....8  
 Kaspersky Lab .....58  
 Kaspersky Lab ZAO .....58

**M**

MAIN WINDOW .....11

**N**

NETWORK PROTECTION STATUS .....17

**P**

PROTECTION STATUS.....17

**R**

REAL-TIME PROTECTION STATUS.....17  
     CRITICAL .....17  
     OK .....17  
     WARNING .....17  
 Reports.....49  
     automatic delivery.....49, 51  
     saving to file.....49, 51  
     viewing.....49, 50

**S**

SECURITY MESSAGE .....17  
     LIST .....17  
 Service provider's administrator .....28  
 SERVICE PROVIDER'S ADMINISTRATOR .....8  
 SESSION .....55  
     LOG OFF.....55  
 SOFTWARE REQUIREMENTS .....10  
 SSL .....8

**U**

Update Agents .....57

**W**

Web browser .....13  
 WEB BROWSER .....8, 10  
 WEB INTERFACE.....8  
 Web portal  
     address.....13  
 WEB PORTAL.....8