Kaspersky Security Center Web-Console

User Guide

CONTENTS

Dear User,

Thank you for choosing our product. We hope that you will find this documentation useful and that it will provide answers to most questions that may arise.

This document may be amended without prior notice. You can find the latest version of this document at the Kaspersky Lab website, at http://www.kaspersky.com/docs.

Kaspersky Lab assumes no liability for the content, quality, relevance, or accuracy of any third-party materials used herein, or for any potential harm associated with the use of such materials.

Document revision date: 12/12/2012

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

ABOUT THIS GUIDE

This document provides information about Kaspersky Security Center Web-Console and instructions on proper use of the application.

This document is aimed at technical specialists (administrators) in organizations where a security system built on Kaspersky Lab solutions is used as a service (provided by a network protection service provider).

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

IN THIS SECTION:

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 pages of the Kaspersky Security Center Web-Console web portal.

Connecting to Administration Server (see page 13)

This section provides instructions on how to get prepared for connection and how to connect to Administration Server using Kaspersky Security Center Web-Console.

Network protection status (see page 15)

This section provides instructions on how to find information on the status of the protection system covering networked computers managed by Administration Server to which the application is connected.

Managing computers (see page 21)

This section provides information on how to view lists of computers on your network and their respective properties.

DOCUMENT CONVENTIONS

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

Table 1. Document conventions

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

KASPERSKY SECURITY CENTER WEB-CONSOLE

Kaspersky Security Center Web-Console is a web application designed to manage the status of the security system of an organization's network protected by Kaspersky Lab applications.

Using the application, you can do the following:

- Manage the status of the organization's security system
- Install Kaspersky Lab applications to computers on your network and manage installed applications
- Manage policies and tasks created for computers on your network
- View reports on the security system status
- Manage the delivery of reports to interested parties: system administrators and other IT specialists

Kaspersky Security Center Web-Console runs on the side of the service provider that provides protection to your network. The protection service 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 figure below shows how Kaspersky Security Center Web-Console works.

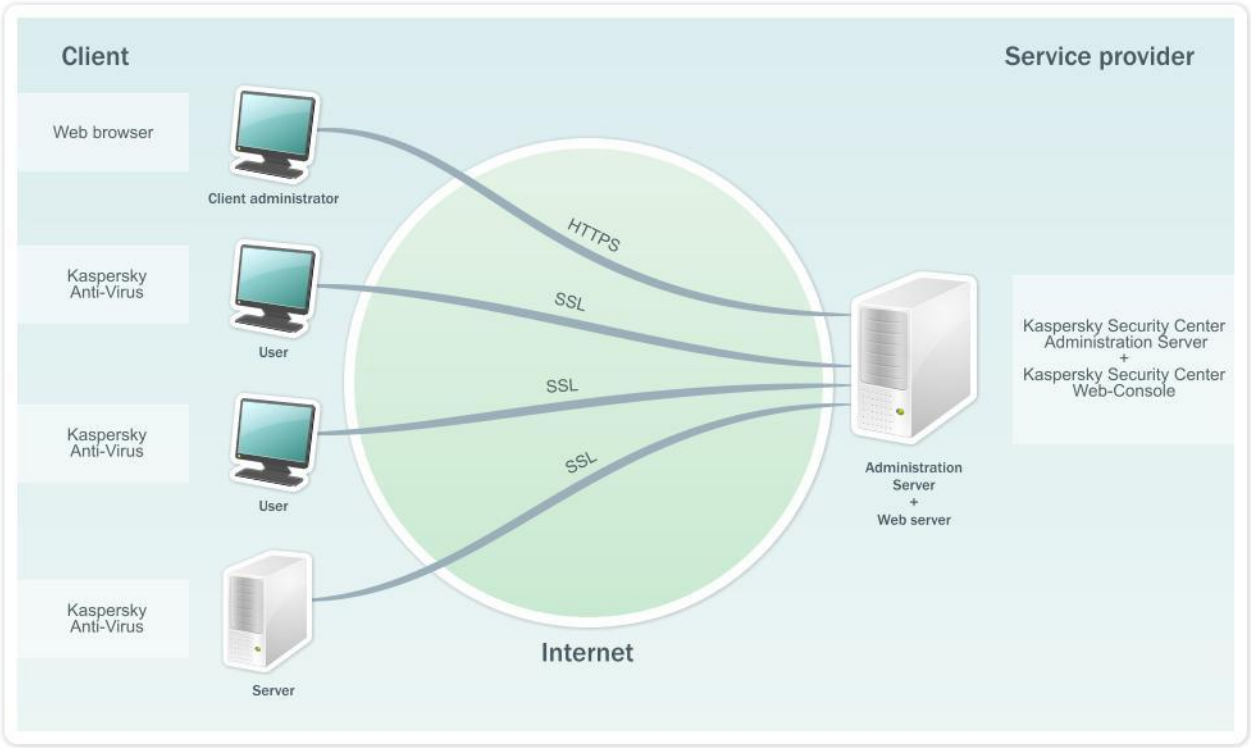

Figure 1. Operating layout

Kaspersky Security Center Web-Console interacts with Kaspersky Security Center Administration Server, which is located at the protection service provider. Administration Server is an application designed for managing Kaspersky Lab applications installed on computers in your network. Administration Server connects to the computers of your network over channels protected by the Secure Socket Layer (SSL) protocol.

Kaspersky Security Center Web-Console provides a web interface that ensures interaction between your computer and Administration Server over a web browser. When you connect to Kaspersky Security Center Web-Console using your web browser, the latter establishes an encrypted (HTTPS) connection with Kaspersky Security Center Web-Console.

Kaspersky Security Center Web-Console operates as follows:

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 web portal controls to choose a command that you want to run. Kaspersky Security Center Web-Console performs the following operations:

    - If you have chosen a command used for reception of information (for example, to view a list of computers), Kaspersky Security Center Web-Console generates a request for information to Administration Server, receives the required data, and sends them to the web browser in an easy-to-view format.

    - If you have chosen a command used for management (for example, remote installation of an 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 the use of Kaspersky Security Center Web-Console.

You can manage Kaspersky Security Center Web-Console via a 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 later running under one of the following operating systems:
  - Microsoft Windows® XP Professional with Service Pack 2 (SP2) or later installed
  - Microsoft Windows 7
  - Microsoft Windows 8
- Firefox™ 16.0 or 17.0 running under one of the following operating systems:
  - Windows operating system:
    - Microsoft Windows XP Professional with Service Pack 2 (SP2) or later installed
    - Microsoft Windows 7
    - Microsoft Windows 8
  - Linux® 32-bit operating systems:
    - Fedora® 16
    - SUSE Linux Enterprise Desktop 11 SP2
    - Debian GNU/Linux 6.0.5
    - Mandriva Linux 2011
    - Ubuntu Desktop 10.04 LTS
    - Ubuntu Server 12.04 LTS.
  - Linux 64 bit operating systems:
    - Red Hat® Enterprise Linux 6.2 server
    - SUSE Linux Enterprise Desktop 11 SP2
    - SUSE Linux Enterprise Server 11 SP2
    - OpenSUSE Linux 12.2
    - Ubuntu Server 12.04 LTS.
- 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 you have established a connection to Administration Server, the main window of Kaspersky Security Center Web-Console opens in the web browser (see figure below).

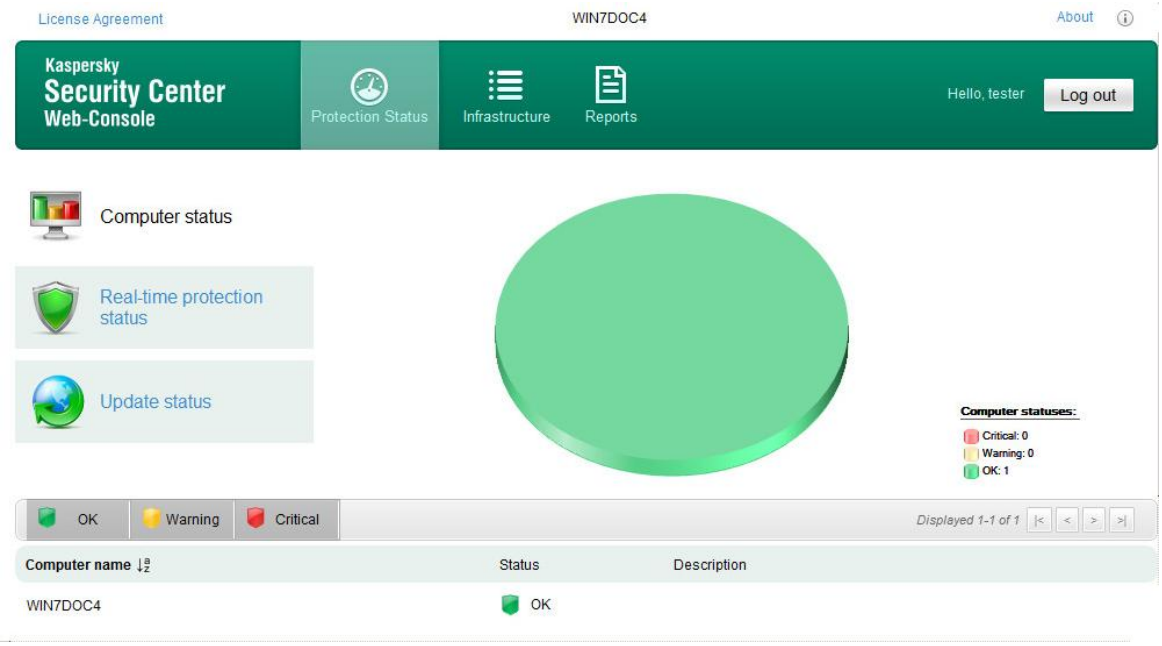

Figure 2. Main application window

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

- The **Protection Status**, **Infrastructure**, and **Reports** tabs — to access the main features of the application.
- Icon — to get context-sensitive help.
- The **Change password** link — to change the password of the account.
- The **Exit** button — to log off the application.
- **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).
- **About**—Link to the application information page.

  Links can be modified by the service provider's administrator. Some links may be missing.

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. In the top part of the tab you can select one of the following sections: **General status**, **Real-time protection status**, **Update status**. After you select a section, a chart appears on the right showing statistics, while the bottom part of the tab displays a list with information about the statuses of computers.

- **Infrastructure**. Designed for obtaining information about administration groups, computers, and policies and tasks created for them. The informational area of the tab is divided into two parts. The menu contains administration groups. The right part of the informational area contains three second-level tabs: **Policies**, **Tasks**, and **Computers**.

- **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.

SEE ALSO:

CONNECTING TO ADMINISTRATION SERVER

This section provides instructions on how to get prepared for connection and how to connect to Administration Server using Kaspersky Security Center Web-Console.

IN THIS SECTION:

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), Open this URL.

   If you are connecting to Administration Server for the first time, the **License Agreement** window opens in the web browser. If you have connected to Administration Server earlier, a window for entering the user name and password opens in the web browser.
3. If you are connecting to Administration Server for the first time, perform the following operations in the **License Agreement** window:

   a. Read through the License Agreement. If you accept all of its terms, select the **Accept terms of the License Agreement** check box.

   b. Click the **Next** button.

   In the web browser, a window opens, prompting you to enter your user name and password.
4. In the **User name** text box enter your account name.
5. In the **Password** text box, enter the password of your account.
6. In the **Administration Server** field enter the name of Administration Server to which you want to connect. Click the **Log in** button.

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

If you have an error returned after attempting to connect to Administration Server, contact the service provider administrator to solve the issue.

NETWORK PROTECTION STATUS

Kaspersky Security Center Web-Console allows you to receive information about the status of the protection system covering computers on the network managed by Administration Server.

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

- Computer status – information about the status of computers on 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 *Warning* or *Critical* status is assigned if there are factors that lower the protection level of the computer (such as inactivity of the anti-virus application, outdated databases, or a large number of objects remaining infected). 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 an anti-virus protection component in Kaspersky Lab applications installed on computers in your network.
- Update status — information on the update status of the anti-virus application database on computers in your network.

IN THIS SECTION:

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. Select the **Protection status** tab.

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

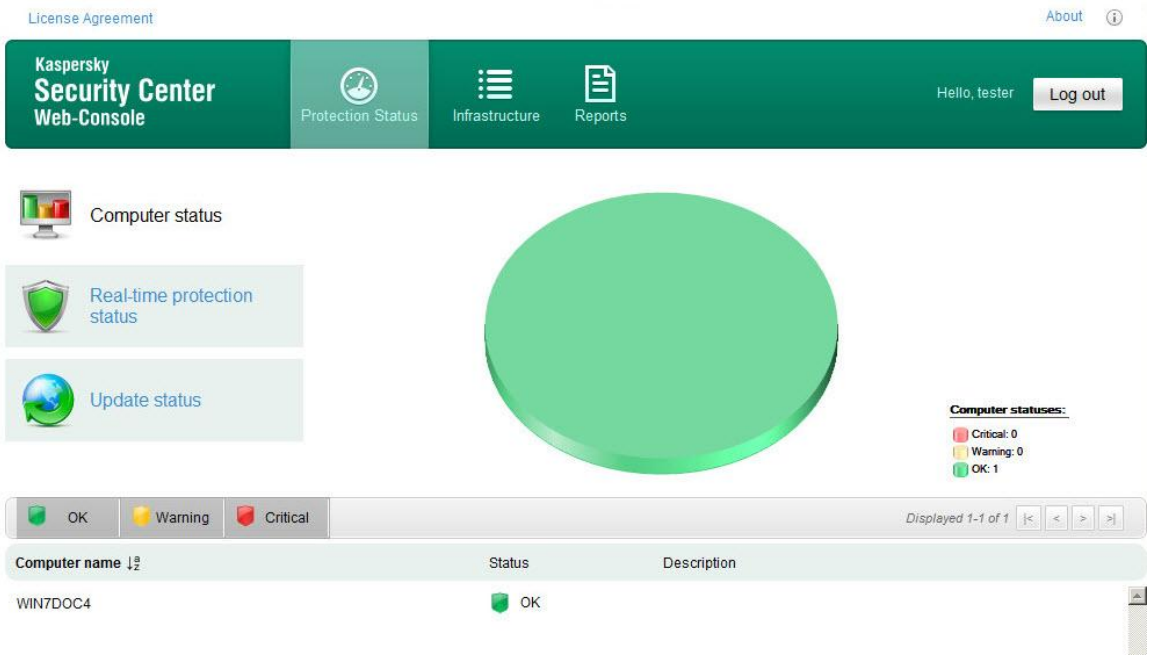

Figure 3. Computers status

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**. Network name of the computer.
- **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 list of the computers.
- Icon — Sorts computer names on the list of computers in ascending or descending alphabetical order.
- Icon — Refreshes the list of computers.

The window with information about the properties of a computer can be opened by clicking the line with the computer name.

SEE ALSO:

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. Select the **Protection status** tab.
3. In the menu, click **Real-time protection status** (see the following figure).

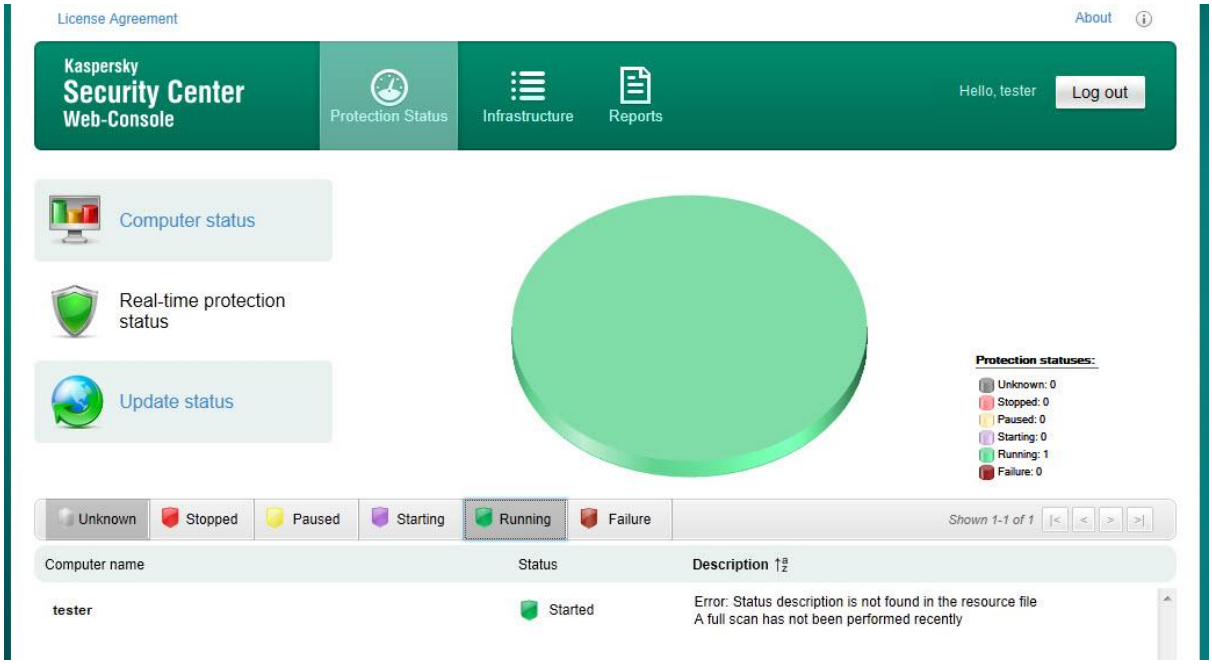

Figure 4. Real-time protection status

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

The chart shows the numbers and the percentages of computers where the protection component 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**. Network name of the computer.
- **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 term expired*).

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

- **Unknown** button – Displays computers with *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.
- Buttons  — Goes to next / previous, first / last page of the list of computers.
- Icon  — Sorts computer names on the list of computers in ascending or descending alphabetical order.
- Icon  — Refreshes the list of computers.

The window with information about the properties of a computer can be opened by double-clicking the line with the computer name.

SEE ALSO:

About computers. About administration groups 21

Viewing computer properties 23

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. Select the **Protection status** tab.

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

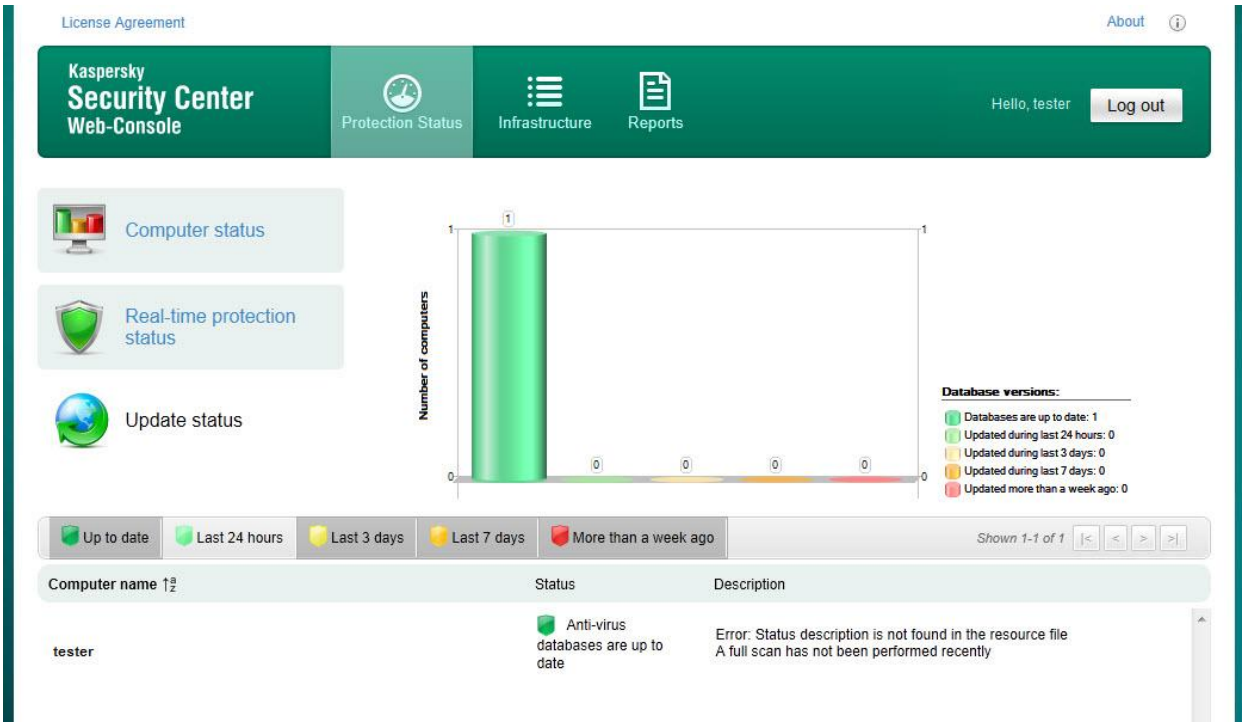

Figure 5. Update status

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**. Network name of the computer.
- **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 *Up to date* status.
- **Last 24 hours** button – Displays computers with *Last 24 hours* status.
- **Last 3 days** button – Displays computers with *Last 3 days* status.

- **Last 7 days** button – Displays computers with *Last 7 days* status.
- **More than a week ago** button – Displays computers with *More than a week ago* status.
- Buttons  — Goes to next / previous, first / last page of the list of computers.
- Icon  — Sorts computer names on the list of computers in ascending or descending alphabetical order.
- Icon  — Refreshes the list of computers.

The window with information about the properties of a computer can be opened by double-clicking the line with the computer name.

SEE ALSO:

MANAGING COMPUTERS

This section provides information about computers on your network and administration groups and details on how to view lists and properties of computers.

IN THIS SECTION:

ABOUT COMPUTERS. ABOUT ADMINISTRATION GROUPS

The security status of computers in your network is managed by Administration Server of your 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 to a networked 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 your networked computers 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 receive information about managed computers from Administration Server: view the list of computers and the properties of managed computers.

SEE ALSO:

VIEWING A LIST OF COMPUTERS

You can view lists of your networked computers managed by Administration Server. You can also view the lists of managed computers for each of the administration groups separately.

To view a list of computers:

1. Open the main application window (see section "Application interface" on page 11).
2. Select the **Infrastructure** tab.
3. In the window that opens, select the **Computers** tab.
4. 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 the list of all managed computers, select the **Managed computers** group.
   - If you want to view the list of managed computers in a particular administration subgroup, select one from the groups tree located under the **Managed computers** administration group.

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

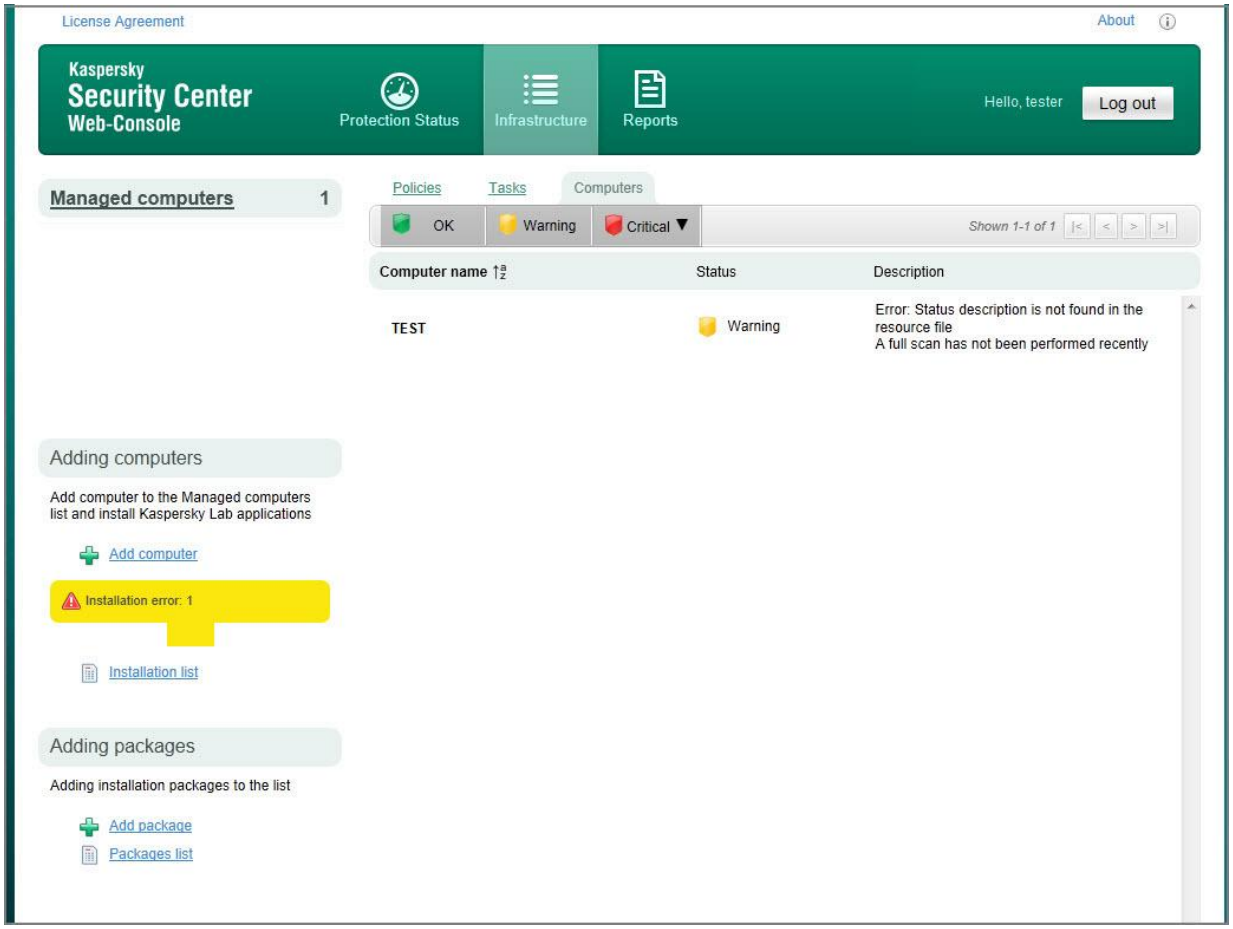

Figure 6. Viewing a list of computers

The list of computers contains the following information:

- **Computer name**. Network name of the computer.
- **Status**. 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 paused* or *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 list of the computers.
- Icon — Sorts computer names on the list of computers in ascending or descending alphabetical order.
- Icon — Refreshes the list of computers.

The window with information about the properties of a computer can be opened by clicking the line with the computer name.

SEE ALSO:

VIEWING COMPUTER PROPERTIES

To view computer properties:

1. Open the main application window (see section "Application interface" on page 11).
2. Select 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 select a computer for which you want to view the properties, and click the line with the computer name to open the window with information about the computer properties (see figure below).

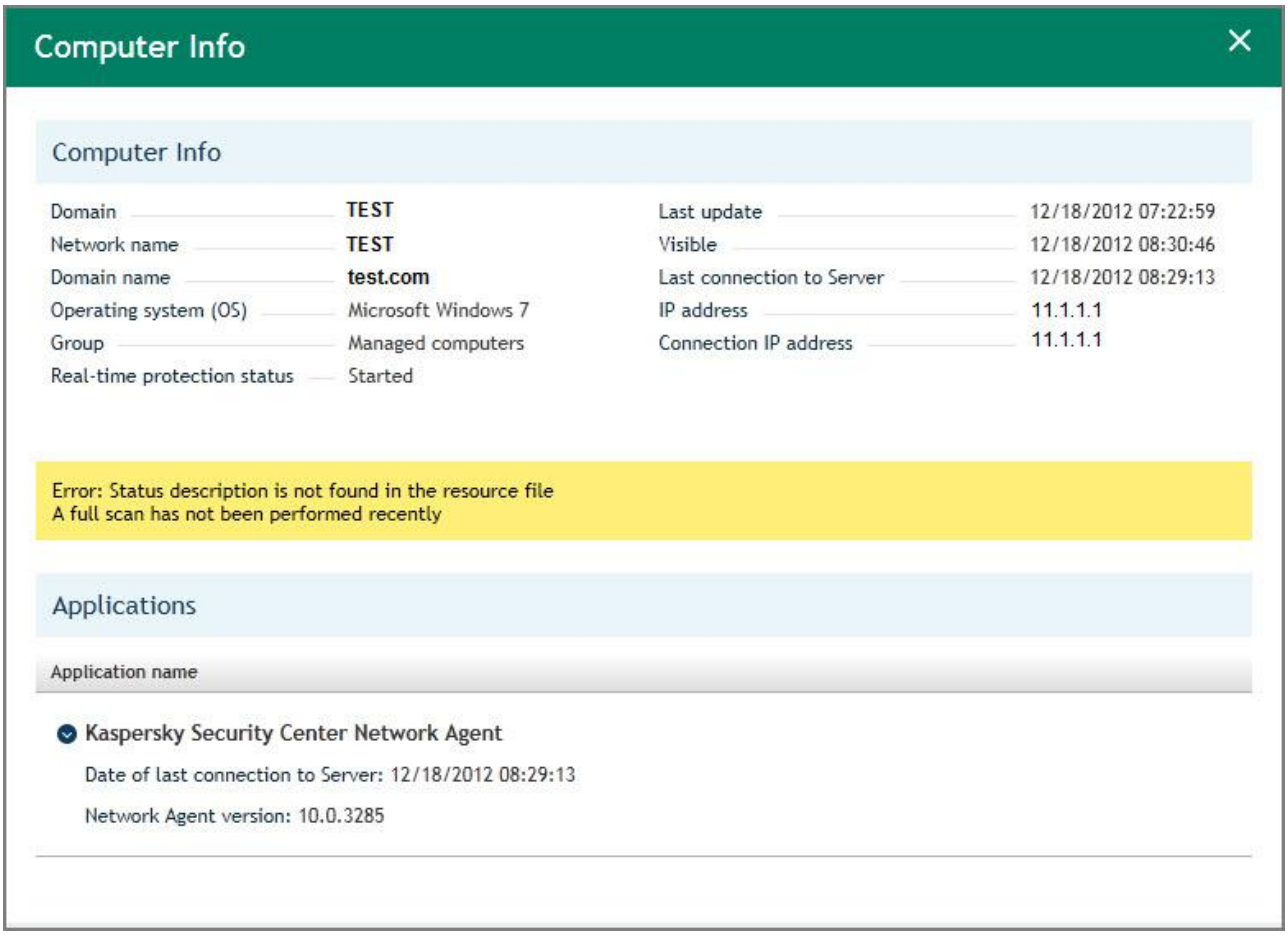

Figure 7. Viewing computer properties

The computer property information appears in two categories.

The top part of the window provides information about the following properties of the computer:

- **Domain**. Name of the network domain where the computer is registered.
- **Network name**. Network name of the computer. 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>.
- **Operating system (OS)**. Type of operating system installed on the computer.
- **Group**. Name of the administration group to which the computer belongs.
- **Real-time protection status**. Status of real-time protection of the computer.
- **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 and time of last connection to Administration Server.
- **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.
- 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*.

The lower part contains the **Applications** section providing information about Kaspersky Lab applications installed on the computer.

The **Applications** section is displayed only if any Kaspersky Lab applications have been 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 the properties of an application, you can use the following interface elements:

- Icon – opens the information section that contains the properties of an application.
- Icon — closes the information section that contains the properties of an application.

SEE ALSO:

About computers. About administration groups.....21

Viewing a list of computers.....21

INSTALLING APPLICATIONS TO NETWORKED COMPUTERS

This section provides instructions on how to install Kaspersky Lab applications and third-party applications to computers on an organization's network in remote installation and local installation modes.

IN THIS SECTION:

ABOUT INSTALLING APPLICATIONS

Using Kaspersky Security Center Web-Console, you can install Kaspersky Lab applications and third-party applications to computers on your network. The list of applications available for installation is created by your service provider's administrator.

There are two ways of installing an application:

- *Remote installation* (referred to as remote installation mode). Remote installation allows you to install an application to several computers on your network at once. You can run and control remote installation through the application web portal.

- *Local installation* (referred to as local installation mode). Local installation is required, for example, in case remote installation fails. You can allow enterprise network users to perform unassisted local installation of applications to their computers.

Applications that are available for installation, are stored on Administration Server as installation packages (see section "About installation packages" on page 26).

SEE ALSO:

ABOUT UPDATE AGENT

Before installing Kaspersky Lab applications and third-party application to computers on your network in remote installation mode, you should assign a computer from your network to be the *update agent*. Update agent is a computer acting as an intermediate relay for distribution of application updates and installation packages within an administration group.

An update agent should meet the following requirements:

- To remain active permanently or the most part of time
- To have a stable access to the Internet and to the rest of computers within the administration group where it distributes updates
- Kaspersky Anti-Virus should be installed on it.

Only after you have assigned one of the computers on your network to be the update agent and installed Kaspersky Anti-Virus to it (see section "Defining an Update Agent" on page 27), you can install applications to other computers on your network in remote installation mode.

SEE ALSO:

ABOUT INSTALLATION PACKAGES

Installation package is a dedicated executable file intended for installation of an application to client computers. An installation package is created based on files included in the application distribution package; it contains a collection of settings required to install the application and ensure its proper functioning immediately after the installation. Parameter values correspond to application defaults.

Installation packages are created and distributed by the service provider administrator.

Installation packages are used for remote installation of Kaspersky Lab applications and third-party applications to client computers through the remote management system called Kaspersky Security Center Web-Console (see section "Remote installation mode" on page 27).

You can install Kaspersky Lab applications and third-party applications to computers on your network in local installation mode (see section "Local installation mode" on page 32), as well as allow users of your network to perform unassisted installation of applications to their computers. To do this, you can use Kaspersky Security Center Web-Console to publish installation packages of applications.

SEE ALSO:

REMOTE INSTALLATION MODE

The remote installation mode allows installing Kaspersky Lab applications and third-party applications to several computers on your network simultaneously.

To activate the remote installation feature, you should first assign one of the computers on your network to be the update agent and install Kaspersky Anti-Virus to it (see section "Defining an Update Agent" on page 27). After that, you will be able to run remote application installation to computers on your network.

Kaspersky Security Center Web-Console performs remote installation of applications in background mode. During remote installation you can use other features of the application, as well as view information about the status of remote installation for each of the computers on which remote installation has been started.

IN THIS SECTION:

DEFINING AN UPDATE AGENT.

After you have selected a computer on your network to act as the update agent, you should install Kaspersky Anti-Virus to it, using the distribution package included in Kaspersky Security Center Web-Console. The first installation of Kaspersky Anti-Virus is performed locally. After you have installed Kaspersky Anti-Virus to the computer, it becomes the update agent automatically. Using the update agent, you can manage installation and updates of Kaspersky Lab applications and third-party applications on remote computers on your network.

To install Kaspersky Anti-Virus to a computer and assign that computer to be the update agent:

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

   The Application Setup Wizard opens, showing the Welcome page.
4. Click the **Install locally on each computer using distribution package** button.

   The **Select distribution package to download** window opens.

   If the application has detected no published installation packages, you will be prompted to publish installation packages (see section "Publishing installation packages" on page 32). After installation packages are published, the application installation continues.
5. Download the Kaspersky Anti-Virus distribution package to your computer. and click the **Download** button next to the application name.
6. Click the **Finish** button. The Application Setup Wizard closes.
7. Copy (using, for example, an external medium or the network) the downloaded Kaspersky Anti-Virus distribution package to the computer on your network that you have assigned the update agent. Install Kaspersky Anti-Virus from the distribution package, following the Distribution Package Installation Wizard's instructions.

After Kaspersky Anti-Virus is successfully installed to the update agent, this computer will be automatically added to the **Managed computers** administration group. The option of remote application uninstallation becomes available in the Application Setup Wizard at the next startup.

The update agent is displayed on the list of computers the next time you log on to Kaspersky Security Center Web-Console web portal or refresh the list.

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

INSTALLING AN APPLICATION REMOTELY

To install an application to your networked computers in remote installation mode:

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

   The Application Setup Wizard opens, showing the Welcome page.
4. Click the **Install to one or more computers in network using installation package** button.

   The **Select installation package** window opens.
5. In the list, select the installation package of an application that you want to install, and click the **Next** button.

   A window opens, showing a list of computers on your network to which you can install the application.

   If you have assigned none of the computers in your network to be the update agent and have not installed Kaspersky Anti-Virus to none of them, no computers from your network are displayed on the list of computers in the Application Setup Wizard window. In this case, you cannot run remote installation of the application to computers on your network.
6. Select the check boxes for computers to which you want to install the application. If you want to install the application to all computers on the list, select the **Computer name** check box. Click **Next**.

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

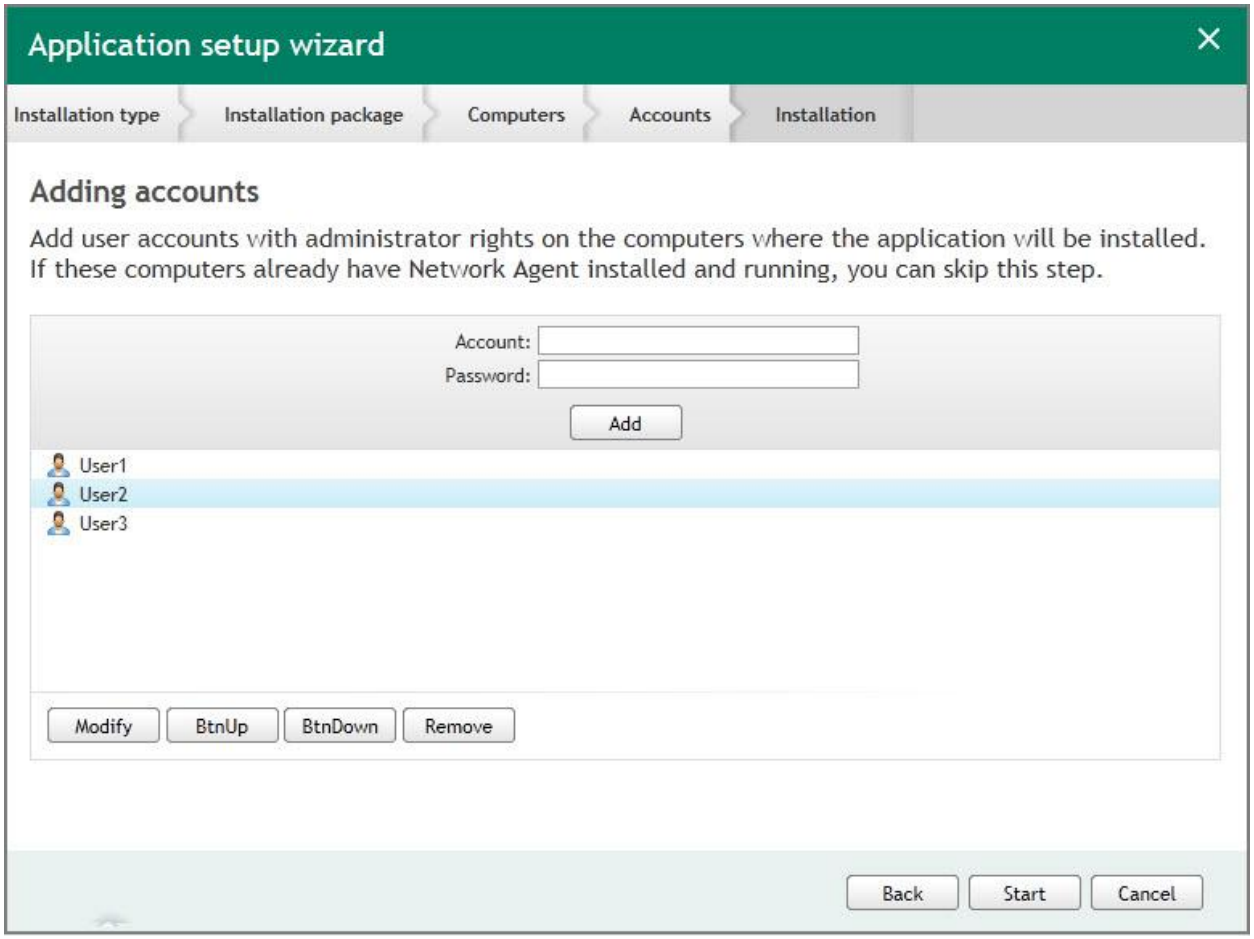

Figure 8. Application Setup Wizard. Adding accounts

- 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 on the list of accounts in the lower part of the window.

- To modify settings of an account:

  a. In the list select an account and click the **Edit** 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).

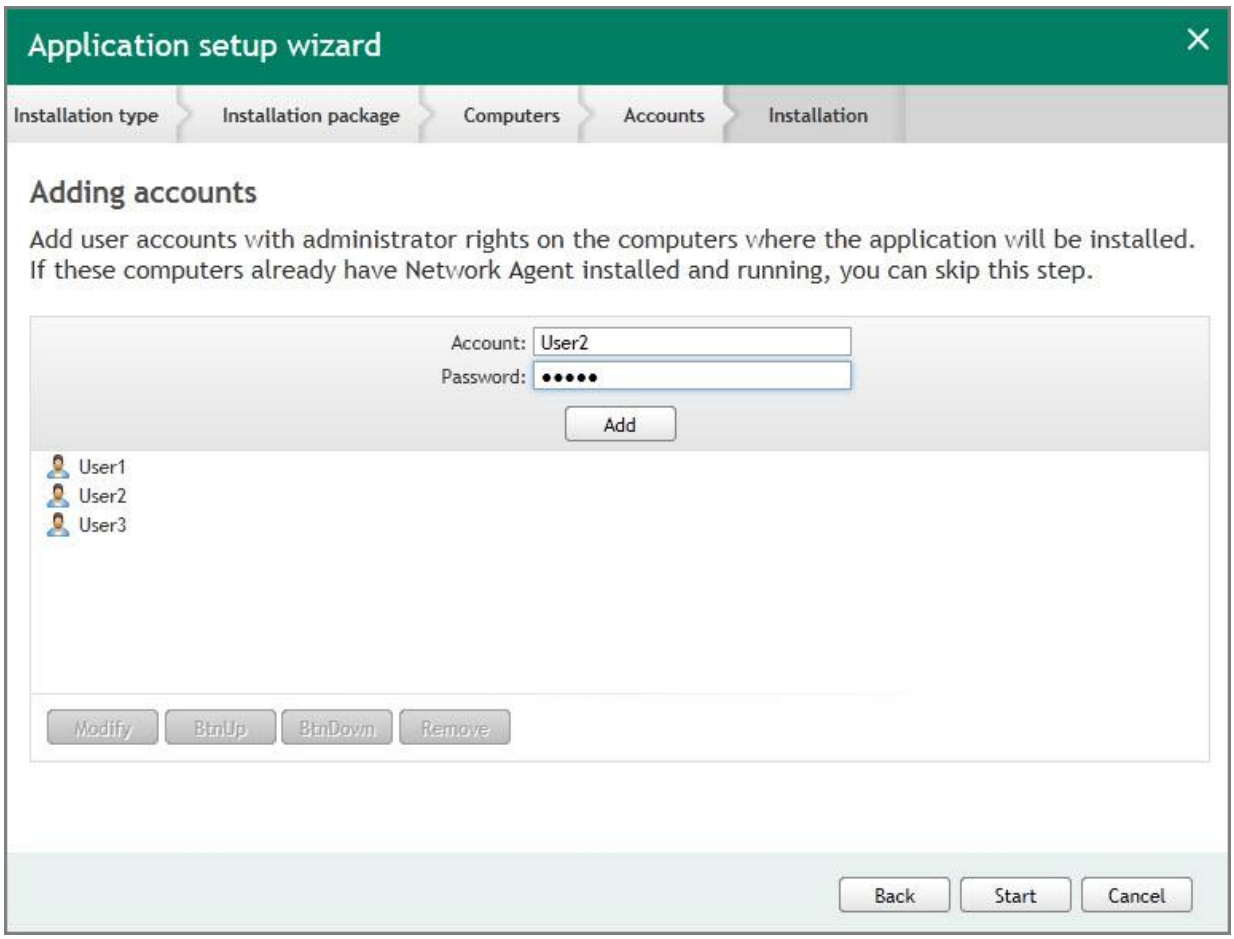

Figure 9. Application Setup Wizard. Modifying an account

The new name and password of the selected account will be saved.

- 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 remote application installation by clicking the **Start** button.

   The remote installation starts on the computers you selected. The **Installing <Application name> to the following computers** window opens, containing a list of tasks of application installation to selected computers of your network.

   You can view the list of installation tasks using the following interface elements:

   - Icon – Sorts the list of installation tasks 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 information about the selected computer.

The section of information about the computer on which remote application installation has been run, contains the following information:

- **Computer name**. Network name of the computer.
- **Status**. Application installation status. 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 exit the Application Setup Wizard, click the **Finish** button. The installation tasks keep on running.

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

Remote application installation may return an error: for example, if another such application has been already installed to the computer. Installation tasks that have returned an error, are displayed on the list of tasks with the *Installation error* status. If remote application installation to one or more computers returns an error, you can install the application locally.

You can run only one remote installation task at once. If you run one more remote installation task before the current remote installation completes, the latter will be stopped.

SEE ALSO:

VIEWING INFORMATION ABOUT THE STATUS OF REMOTE INSTALLATION OF AN APPLICATION

During remote installation of an application, you can view information about the installation status for each of the computers on which remote installation has been started.

To view status information about remote installation of an application:

1. Open the main application window (see section "Application interface" on page 11).
2. Select the **Infrastructure** tab.

   If at least one remote installation of an application has been started, the panel on the left displays the **List of installations** link.

3. Click the **List of installations** link to open the **List of active installations** window. The **List of active installations** window contains a list of application installations to computers on your network.

Computers on the list of installations can have the following statuses:

- *Installation in progress* — remote installation of the application has not yet completed.
- *Installation error* — remote installation of the application has completed with an error. We recommend that you install the application manually.

SEE ALSO:

LOCAL INSTALLATION MODE

You can install Kaspersky Lab applications and third-party applications to computers on your network in local installation mode. Local installation of applications can be performed in one of the two following ways:

- Manual installation with the distribution package. You can download the application distribution package to a computer and perform *installation manually*, following the Distribution Package Installation Wizard's instructions. Manual installation (also referred to as manual installation mode) requires your immediate participation in application installation to each computer. You can allow users of your network to perform unassisted manual installation of applications to their computers, by moving distribution packages to a shared network folder. A user account on a computer or in a network domain should have rights required for installation of applications to the target computer.

- Installation using an installation package. To perform application installation in this way, you should publish the application installation package. After publishing, Kaspersky Security Center Web-Console provides a link to the published installation package. Then you can use this link to download the published installation package to the computer and run it. After running the published installation package, the application installation will be performed automatically. You can allow users of your network to perform unassisted installation of applications to their computers using published installation packages; to do this, send users links to published installation packages (for example, by email).

IN THIS SECTION:

PUBLISHING INSTALLATION PACKAGES

To publish installation packages:

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

   A window opens displaying a list of installation packages that you can publish.
4. Select the check boxes for installation packages that you want to publish. If you want to publish all of the installation packages on the list, select the check box next to the **Installation package name** header.

5. Click the **Publish** button.

   The statuses of the installation packages that you have selected changes to *Publishing*. Publishing of the selected installation packages starts.

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

Publishing of installation packages continues in automatic mode. After the publishing completes, the installation packages are added to the list of published installation packages.

Published installation packages are stored on Administration Server. Kaspersky Security Center Web-Console provides links for downloading published installation packages. You can send those links to users of your network.

SEE ALSO:

About installation packages.....26

Canceling installation package publishing.....33

Viewing the list of published installation packages 33

VIEWING THE 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. Select the **Infrastructure** tab.
3. Click the **List of packages** link in the left part of the window to open the **List of installation packages** window.

   A window opens showing a list of published installation packages.

The list contains the following information about published installation packages:

- **Installation package name**. The name of the published installation package.
- **Installation package URL**. A URL used to download the published installation package from the local network.

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

You can send links to published installation packages to users of your network (for example, by email). Users of your network can use them for downloading published installation packages to their computers and for installing applications.

SEE ALSO:

About installation packages.....26

CANCELING INSTALLATION PACKAGE PUBLISHING

You can cancel publishing of an installation package (for example, if its version has gone out of date).

To cancel publishing of an installation package:

1. Open the main application window (see section "Application interface" on page 11).
2. Select the **Infrastructure** tab.

3. Click the **List of packages** link in the left part of the window to open the **List of installation packages** window.

   A window opens showing a list of published installation packages.

4. On the list, find the installation package for which you want to cancel publishing, and click the **Block access** button in the corresponding line.

   The text *package deleted, access blocked* appears in the line. Publishing of the selected installation package will be canceled. The package becomes unavailable for download.

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

After publishing is canceled, the installation package is deleted from Administration Server and becomes unavailable for download. The link to the installation package becomes inactive.

SEE ALSO:

About installation packages.....26

INSTALLING AN APPLICATION USING A PUBLISHED INSTALLATION PACKAGE

To install an application a published installation package:

1. Download a published installation package to the computer to which you want the application installed. To do this, use the link received after publishing of the installation package.

   To find the link that you should click to download the published installation package from the local network, open the list of published packages (see section "Viewing the list of published installation packages" on page 33).

2. Run the published installation package. After you have run it, the installation will be performed automatically.

3. Wait until the application installation completes.

INSTALLING AN APPLICATION MANUALLY

To install an application manually:

1. Open the main application window (see section "Application interface" on page 11).

2. Select the **Infrastructure** tab.

3. Click the **Add computer** link in the pane to the left to start the Application Setup Wizard.

   The Application Setup Wizard opens, showing the Welcome page.

4. Click the **Install locally to each computer using downloaded distribution package** button.

   The **Select distribution package to download** window opens.

   If the application has detected no published installation packages, you will be prompted to publish installation packages (see section "Publishing installation packages" on page 32). After installation packages are published, the application installation continues.

5. Select the installation package that you want to install manually To do this, click the **Download** button next to the application name.

6. Click the **Finish** button. The Application Setup Wizard closes.

7. Run the installation package of the application on each of the computers where you want the application installed. Then follow the instructions of the installation package wizard.

Computers to which the application is successfully installed are automatically added to the **Managed computers** administration group.

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

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

SEE ALSO:

About installation of applications 25

Viewing a list of computers..... 21

Connecting to Administration Server..... 14

Defining an Update Agent. 27

MANAGING POLICIES

Policy is a collection of application settings defined for an administration group. By using policies, you can specify common values for the application settings in a centralized manner for all the client computers in an administration group, as well as forbid any changes in the settings to be made locally via the application interface. The policy does not define all the application settings.

Several policies with different values can be defined for a single application. However, there can be only one active policy for an application at a time. There is the capability to activate a disabled policy on a certain event. This means that you can, for example, enforce stricter anti-virus protection settings during virus outbreaks.

The program can run in different ways for different groups of settings. Each group can have its own policy for an application.

Also, policies for mobile users can be created. If connection between Administration Server and a client computer is interrupted, the client computer starts running under the policy for mobile users (if it is defined), or the policy keeps running under the applied settings until the connection is re-established.

After a policy is deleted or revoked, the application continues working with the settings specified in the policy. Those settings can be subsequently modified manually.

IN THIS SECTION:

VIEWING A LIST OF POLICIES

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

To view a list of policies:

1. Open the main application window (see section "Application interface" on page 11).
2. Select the **Infrastructure** tab.
3. In the window that opens, select the **Policies** tab.
4. In the left part of the window select an administration group for which you want to view a list of policies:

A list of policies for the selected administration group is displayed on the screen (see figure below).

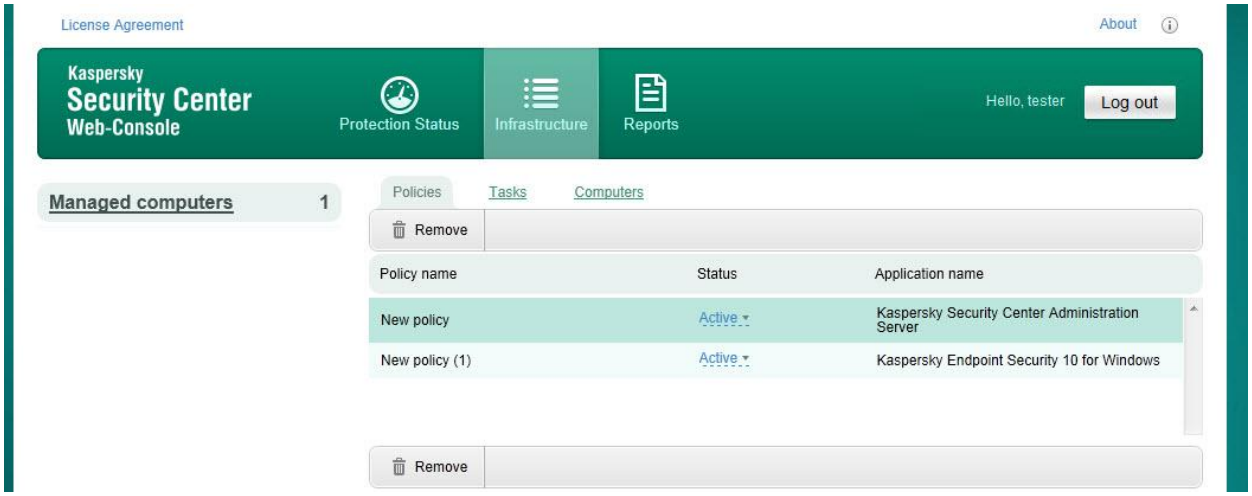

Figure 10. Viewing a list of policies

The list of policies contains the following information:

- Policy name
- Policy status (active, inactive, for mobile users)
- Name of the application for which the policy has been created.

To view information about a specific policy, use the following interface elements to find it on the list:

- Buttons |< < > >| – Goes to the next / previous, first / last page of the list of policies.
- Icon in the column header – Sorts entries on the list of policies by column value in ascending or descending alphabetical order.

ACTIVATING A POLICY

To make a policy active for a selected administration group:

1. In the main application window (see section "Application interface" on page 11), on the **Infrastructure** tab select the **Policies** tab.
2. From the list select a policy that you want to activate.
3. From the dropdown list, in the **Status** column select the **Active** value.

As a result, the policy becomes active for the selected administration group.

When a policy is applied to a large number of clients, both the load on the Administration Server and the network traffic increase significantly for a period of time.

APPLYING A ROAMING POLICY

A roaming policy takes effect on a computer in case it is disconnected from the enterprise network.

To apply the selected roaming policy,

1. In the main application window (see section "Application interface" on page 11), on the **Infrastructure** tab select the **Policies** tab.
2. From the list select a policy that you want to apply to mobile users.
3. From the dropdown list, in the **Status** column select the **For mobile users** value.

As a result, the policy applies to the computers in case they are disconnected from the enterprise network.

DELETING A POLICY

To delete a policy:

1. In the main application window (see section "Application interface" on page 11), on the **Infrastructure** tab select the **Policies** tab.
2. From the list select the policy that you want to delete.
3. Click the **Delete** button.
4. In the window that opens, confirm the operation by clicking the **Yes** button.

As a result, the policy will be deleted from the list.

MANAGING TASKS

Administration Server manages applications installed on client computers, by creating and running tasks. Tasks are required for installing, launching and stopping applications, scanning files, updating databases and software modules, and taking other actions on applications.

Any number of tasks can be created for each application.

You can start and stop tasks, view run results, and delete tasks.

The run results of tasks are saved both on Administration Server in a centralized manner and locally on each client computer.

IN THIS SECTION:

VIEWING A LIST OF TASKS

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

To view a list of tasks:

1. Open the main application window (see section "Application interface" on page 11).
2. Select the **Infrastructure** tab.
3. In the window that opens, select the **Tasks** tab.
4. In the left part of the window select an administration group for which you want to view a list of tasks:

A list of tasks for the selected administration group is displayed on the screen (see figure below).

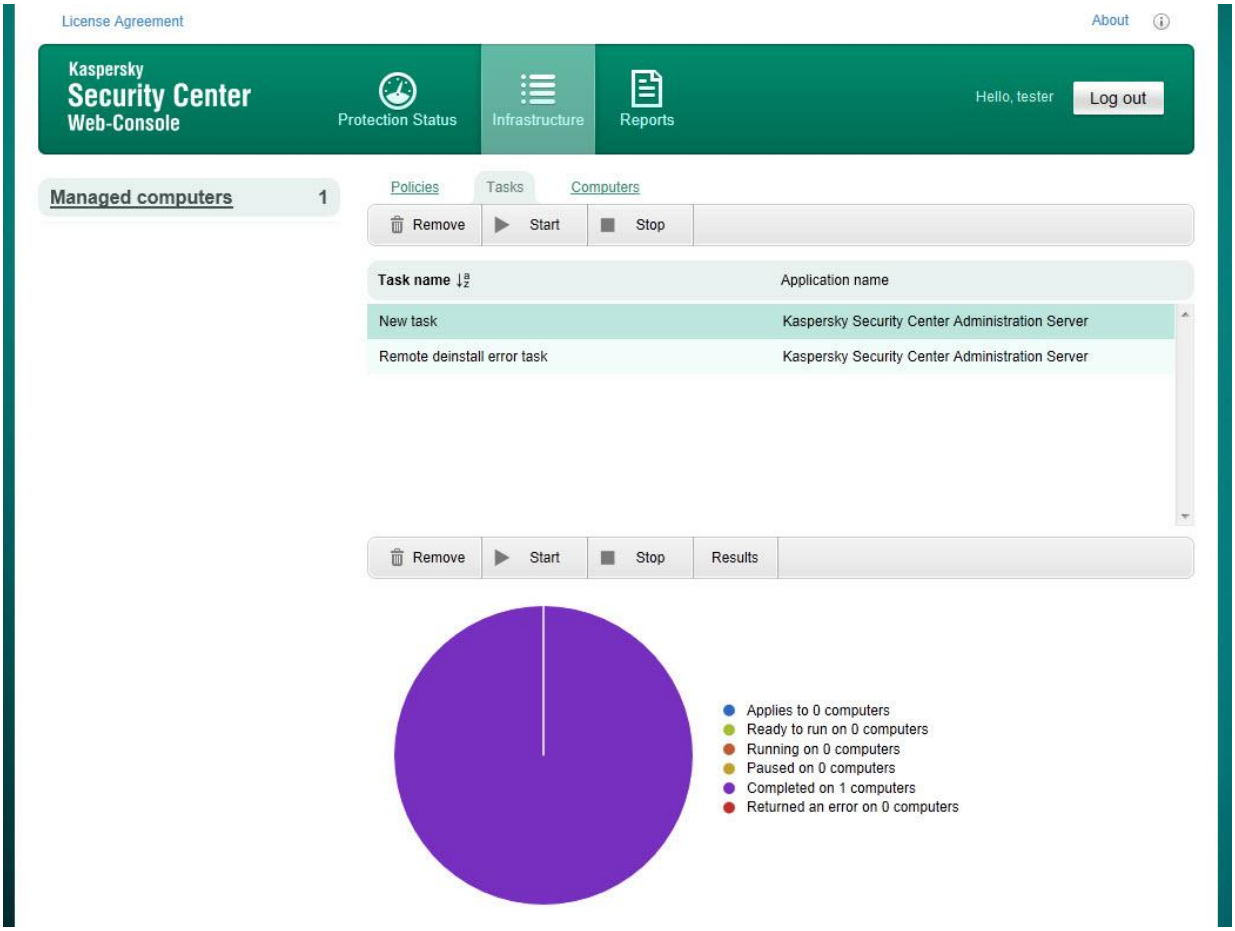

Figure 11. Viewing a list of tasks

The list of tasks contains the following information:

- Task name
- The name of the application for which the task has been created.

The bottom part of the window displays the run statistics for the task selected from the list of tasks.

To view information about a specific task, use the following interface elements to find it on the list:

- Buttons |< < > >| – Goes to the next / previous, first / last page of the list of tasks.
- Icon in the column header – Sorts entries on the list of tasks by column value in ascending or descending alphabetical order.

STARTING AND STOPPING A TASK MANUALLY

To start or stop a task manually:

1. In the main application window (see section "Application interface" on page 11), on the **Infrastructure** tab select the **Tasks** tab.
2. From the list select a task that you want to start or stop.
3. Click the **Start** or **Stop** button.

   As a result, the task will be started or stopped.

Tasks are launched on a client only if the application for which the task was created is running. When the application is not running, all running tasks are canceled.

VIEWING TASK RUN RESULTS

To view the run results of a task:

1. In the main application window (see section "Application interface" on page 11), on the **Infrastructure** tab select the **Tasks** tab.
2. From the list of tasks select one for which you want to view the run results.
3. Click the **View results** button.

The run results for the selected task are displayed in the window that opens.

DELETING TASKS

To delete a task, perform the following steps:

1. In the main application window (see section "Application interface" on page 11), on the **Infrastructure** tab select the **Tasks** tab.
2. From the list of tasks select one that you want to delete.
3. Click the **Delete** button.
4. In the window that opens, confirm the task deletion by clicking the **Yes** button.

As a result, the task will be deleted from the list.

WORKING WITH REPORTS

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

IN THIS SECTION:

ABOUT REPORTS

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

Reports provide various information about the status of the protection system covering computers managed by Administration Server.

The list of available reports is created by your service provider's administrator. The list of reports may 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 may need to configure Kaspersky Security Center Web-Console to deliver reports by email to you and other staff members involved in anti-virus protection of your network (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

To view a report:

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

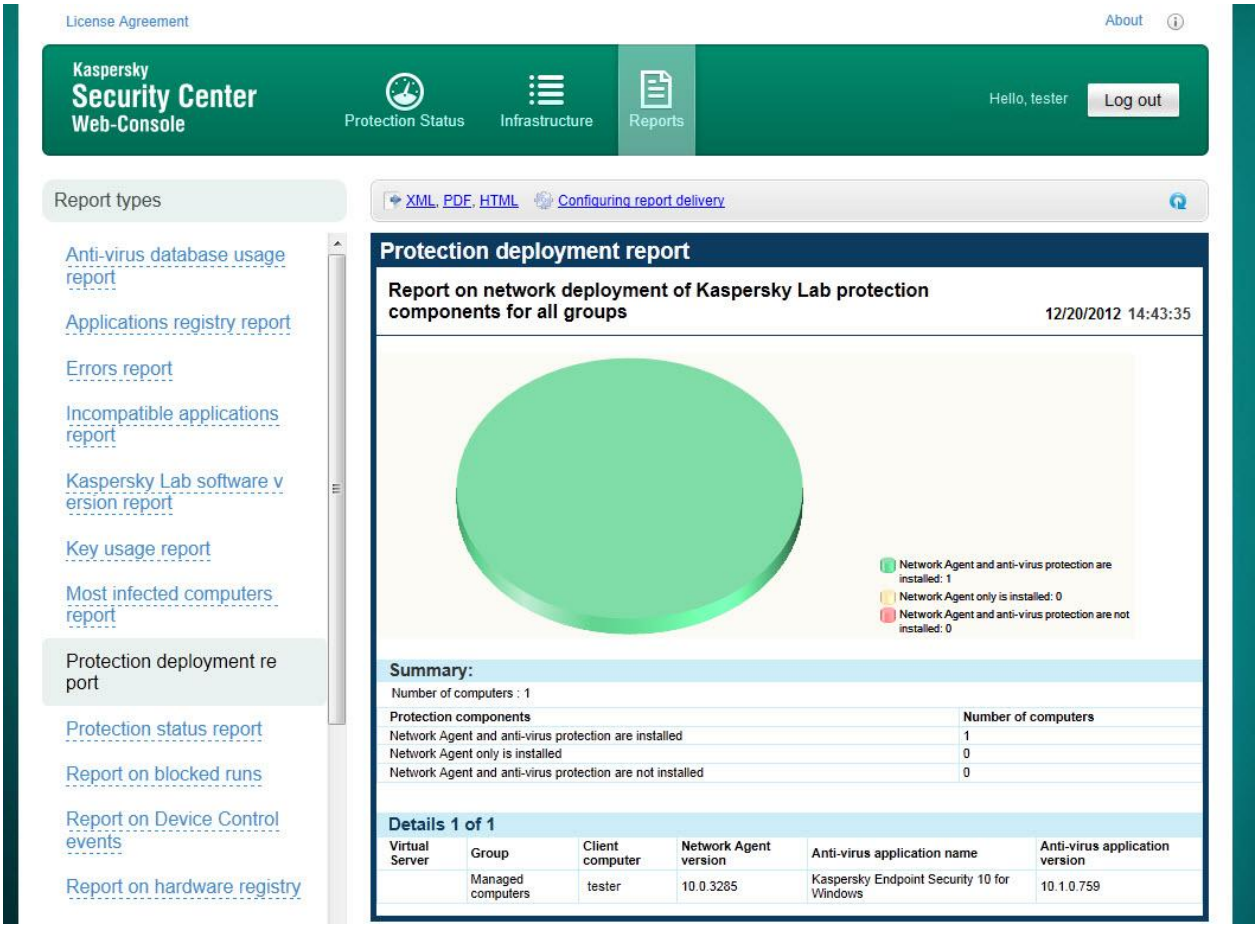

Figure 12. Viewing reports

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 located in the top 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. Select 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. Select the **Reports** tab.
3. Click the link in the upper part of the main window to open the **Configuring reports delivery** window.
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  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 select the email address that you intend to modify.

     The selected email address is displayed in the **Recipient address** field.

  b. Change the email address in the **Recipient address** field and click the  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 in 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 and open the **Change password** window.
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 of the application interface.

To exit the application, you should first log off Kaspersky Security Center Web-Console.

If you exit the web browser without logging off (for example, by closing the window or the web browser tab), the sessions remains active for the next 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 out** link in the top right corner of the window.

  You have just logged off Kaspersky Security Center Web-Console. In the web browser an entry window for user name and password opens (see section "Connecting to Administration Server" on page 14).

GLOSSARY

A

Administration Server

A component of Kaspersky Security Center that centrally stores information about all Kaspersky Lab applications that are installed within the corporate network. It can also be used to manage these applications.

Administration group

A set of computers grouped together in accordance with the performed functions and the Kaspersky Lab applications installed on those machines. Computers are grouped for convenience of management as one single entity. A group can include other groups. A group can contain group policies for each application installed in it and appropriate group tasks.

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 uninstallation of a Kaspersky Lab application by using the remote administration system named Kaspersky Security Center Web-Console. An installation package is created based on special files with the .kpd and .kud extensions that are included in the application distribution package; it contains a set of settings required for application setup and its configuration for normal functioning immediately after installation. Parameter values correspond to application defaults.

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 an anti-virus application to a computer on an organization's network that presumes a manual startup of the installation process from the distribution package of the anti-virus application or a manual startup of a published installation package that has been downloaded to the computer preliminarily.

M

MANAGED COMPUTERS

Corporate network computers that are included in an administration group.

MANUAL INSTALLATION

Installation of an anti-virus application to a computer on an organization's network from the distribution package of the anti-virus application. Manual installation requires an immediate participation of an administrator or another 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, use of keys, and number and types of detected threats.

R

REMOTE INSTALLATION

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

S

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.

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.

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 SPE. 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 a few top Advanced+ awards in a test held by AV-Comparatives, an acknowledged 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 (only for sending probably infected files in archive format)
	http://support.kaspersky.com/virlab/helpdesk.html
	(for queries addressed to virus analysts)
Kaspersky Lab's web forum:	http://forum.kaspersky.com

INFORMATION ON THE THIRD-PARTY CODE

The third-party code was used to create the application.

IN THIS SECTION:

C++ JSON PARSER 4.03

C++ JSON Parser 4.03

The MIT License

FCGI-2.4.1-SNAP-0910052249

fcgi-2.4.1-SNAP-0910052249

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 NOTICE

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

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

Fedora and Infinity design logo are trademarks owned by Red Hat, Inc.

Microsoft, Windows, Windows Vista, and Internet Explorer are trademarks owned by Microsoft Corporation and registered in the United States of America and elsewhere.

Linux is a trademark owned by Linus Torvalds and registered in the United States of America and elsewhere.

Red Hat and Red Hat Enterprise Linux are trademarks owned by Red Hat, Inc. and registered in the United States of America and elsewhere.

Mac OS, Safari, Leopard, Snow Leopard, and Tiger are registered trademarks owned by Apple Inc.

Mozilla and Firefox are trademarks of the Mozilla Foundation.

INDEX

A

C

H

I

J

K

M

N

P

R

S

W