Protecting Systems Using Antiviruses

Module 3

Simplifying Security.

Certified Secure Computer User

Module 3: Protecting System Using Antiviruses

Exam 112-12

Module Objective

This module will familiarize you with:

- The Most Dangerous Computer Viruses of All Time
- Introduction to Antivirus Software
- How Does Antivirus Software Work?
- Antivirus Software 2011
- Steps to Install Antivirus on Your Computer
- How to Test if Antivirus is Working?
- Choosing the Best Antivirus Software
- Configuring McAfee Antivirus
- Configuring Kaspersky PURE
- Guidelines

Module Flow

Introduction to Antivirus Software

How Does Antivirus Software Work?

Choosing the Best Antivirus Software

Steps to Install Antivirus

Configuring McAfee Antivirus

Configuring Kaspersky PURE

Introduction to Antivirus Software

A computer plugged into the Internet is always at **high risk**, and it is always recommended to install antivirus software onto the system. A **computer virus** can degrade the performance of a computer and delete stored computer data. Viruses usually spread through networks by means of download, email, and shared disk. If an infected file is attached to these sources, then the system is likely to become infected upon opening the infected files. Some of the **symptoms** indicating viral infection are **improper functioning** of applications, slow operation, an unusual error message, frequent hanging, frequent re-starting, problems printing, double extension on any attachment, and distorted menus and dialog boxes

An **antivirus program** scans the hard drive and floppy disks to protect the computer against viruses, worms, spywares, Trojans, and more. It ensures that the system is healthy and alerts the person to implement safety measures against harmful attacks. **Regularly update** the antivirus software by subscribing to the updates from antivirus vendors whenever offered. The **virus dictionary** and suspicious behavior approaches are the most widely used approaches by antivirus software to detect malware.

Need for Antivirus Program

Today in the digital domain, loads of data is stored on computers and it has become significant to protect the data. When a PC is connected to the Internet, the PC has to combat different **malicious programs** such as viruses, worms, Trojans, spyware, adware. **Cyber criminals** such as attackers and hackers use these malicious programs as tools to **steal** important **information** such as personal data stored on the computer. These programs pose a **severe threat** to the computer and may destroy its functionality in different ways.

Malicious programs pave their way into one's PC through email attachments and spam email, through USB drives, visiting a fraudulent website, etc. Due to the invasion of malicious programs in cyberspace, antivirus programs have become necessary for computers. If your computer has a **good antivirus program** installed, then the PC is protected and combats all types of malicious programs.

How Does Antivirus Software Work?

Most of the commercial antivirus software use two techniques:

- Using a **virus dictionary** to look for known viruses while examining files
- Detecting **suspicious behavior** from a computer program

Techniques used by antivirus software to scan files in order to identify and eliminate malicious software and other computer viruses include:

Virus dictionary approach:

- While examining files, the antivirus software refers to the **dictionary of known viruses** identified by the author of the antivirus software.
- If a bit of code in the file matches with that of any virus in the dictionary, then the antivirus software can delete the file, repair the file by removing the virus, or quarantine it to make the file inaccessible to other programs.
- To be successful, this approach requires the virus dictionary to be updated with periodic online downloads.
- The antivirus software usually examines files when the OS creates, opens, and closes the files as well as when they are emailed.
- The software can be normally scheduled on the hard disk to regularly examine the files.

Suspicious behavior approach:

- In this approach, the antivirus software **monitors the behavior of all programs** instead of identifying the known viruses.
- Whenever a program with suspicious behavior is found, the software alerts the user and asks what to do.
- This approach provides protection against new viruses that do not exist in virus dictionaries.

Other ways to detect viruses:

- Anti-virus software will try to emulate the beginning of each new executable code that is being executed before transferring control to the executable.
- If the program seems to be a virus or using self-modifying code, then it immediately examines the other executable programs.
- This approach results in more false positives.
- **Sandbox** is another kind of detection method that emulates the OS and runs the executable in this simulation. The sandbox is examined for a virus after the termination of a program. It is performed during on-demand scans.

Antivirus Software 2011

A list of popular antivirus software includes:

Figure 03-01: Antivirus Software

Choosing the Best Antivirus Software

When purchasing an antivirus software, look for certain features and choose the one that can best serve your needs.

The most important things to consider are:

- **Antivirus Scanning**
  - **Antivirus Detection Accuracy:**

    Ensure that antivirus software scans and detects viruses accurately and detects the majority of threats
  - **Scanning Speed:**

    Ensure that the antivirus software can perform the task quickly and efficiently
  - **Resource Utilization:**

    Ensures that the antivirus software utilizes minimal resources and does not affect system performance when scanning the computer
- **Hacker Blocking:**

Prevents other users from gaining unauthorized access and stealing important data such as passwords and other confidential information

- **Bidirectional Firewall:**

  Ensure that the antivirus software is equipped with a software firewall to scan both incoming and outgoing traffic

- **Technical Support:**

  Look for good technical support so issues can be solved easily

- **Parental Controls:**

  Ensure that the antivirus program has parental control features so children can browse the Internet safely

- **Easy Installation (and Easy to Use):**

  The antivirus software should be user-friendly and easy to use

- **On-Demand and Scheduled Scanning:**

  Allows you to schedule a scan according to a user-specified time. Users can schedule the scan daily, weekly, or monthly

- **Automatic Updates:**

  Keeps the user abreast of the latest online threats without the user having to visit the vendor's website

- **Spyware Detection and Prevention:**

  Checks for antispyware components keep spyware at bay

- **Email Scanning:**

  Email protection can monitor POP and SMTP ports and ensure that the emails do not contain a threat to your computer

Steps to Install Antivirus on Your Computer

Most of the antiviruses follow a wizard-driven installation process and necessary components are installed in the system by default. To install antivirus on a system:

- Download the antivirus and launch the installation of antivirus by double clicking the setup file
- Agree to the legal agreement that might appear, click "**I agree**", and then click "**Next**" to continue
- Review all the settings and click next until installation is finished
- Once the installation process is finished, restart your computer

How to Test If Antivirus Is Working

To determine the presence of consistent virus protection, follow these steps:

- Open a new document in **Notepad**.
- Copy the following code into it, and save the file.
  - X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
- Rename the file as **myfile.com**.
- Run the antivirus scan on myfile.com.
- If the antivirus is functioning properly, it will generate a **warning** and immediately delete the file.

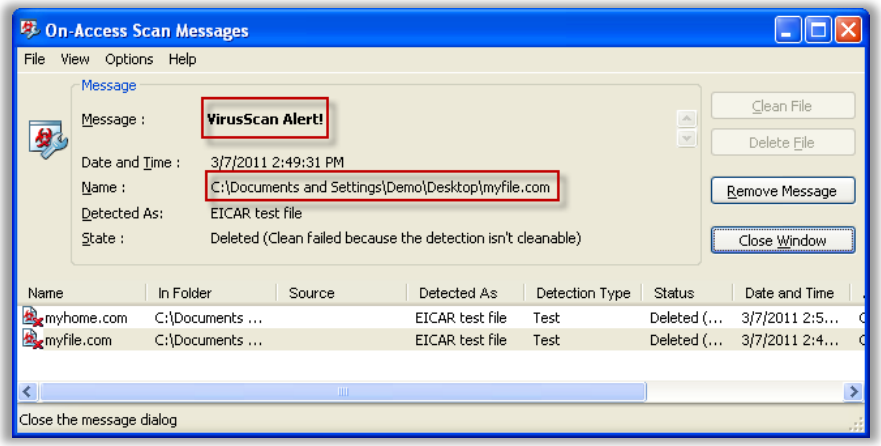

Figure 03-02: On-Access Scan Message

Configuring McAfee Antivirus

- On the Main Security Center Console, click **Real-time Scanning** and select **Scan your PC.**
- After selecting, **Scan your PC,** select any one of the available three scan types (**Run a quick scan, Run a full scan,** or **Run a custom scan**).

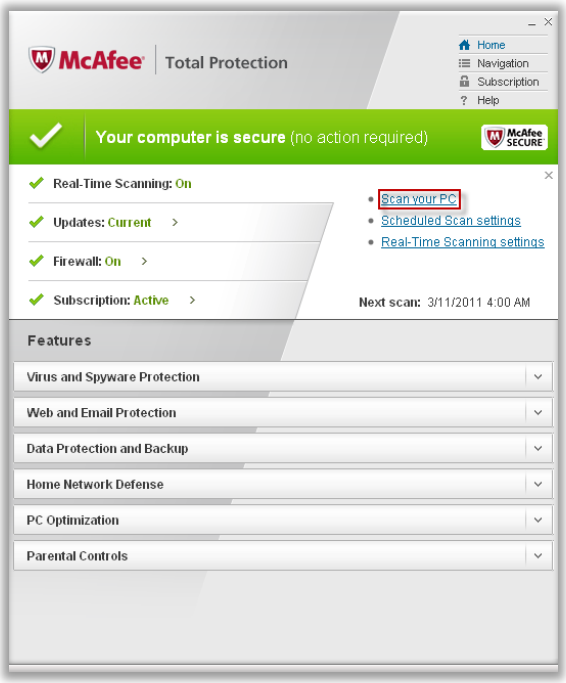

Figure 03-03: Selecting to Scan the PC

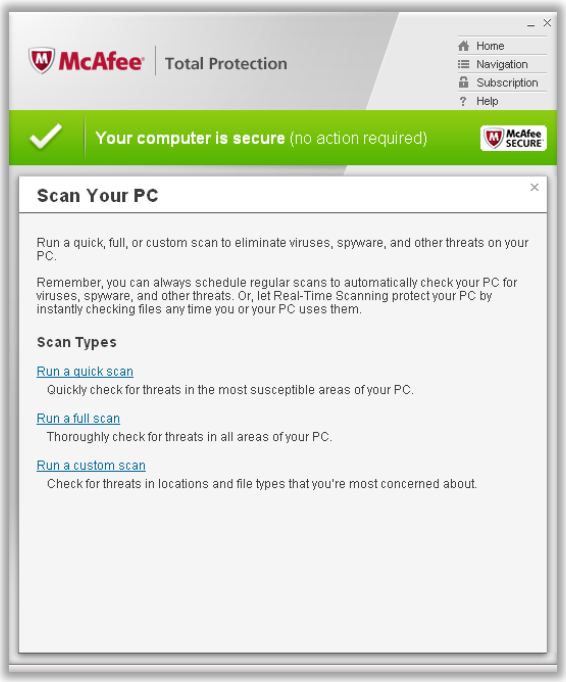

Figure 03-04: Scan Types

- On the Main Security Center Console, click **Real-time Scanning,** select **Schedule Scan Settings,** and decide how often you want to scan. Click **Apply.**
- After selecting **Schedule Scan Settings** and **Real-time Scanning Settings,** select the file types, attachments, and locations that you want the antivirus to scan automatically and protect the computer from threats. Click **Apply.**

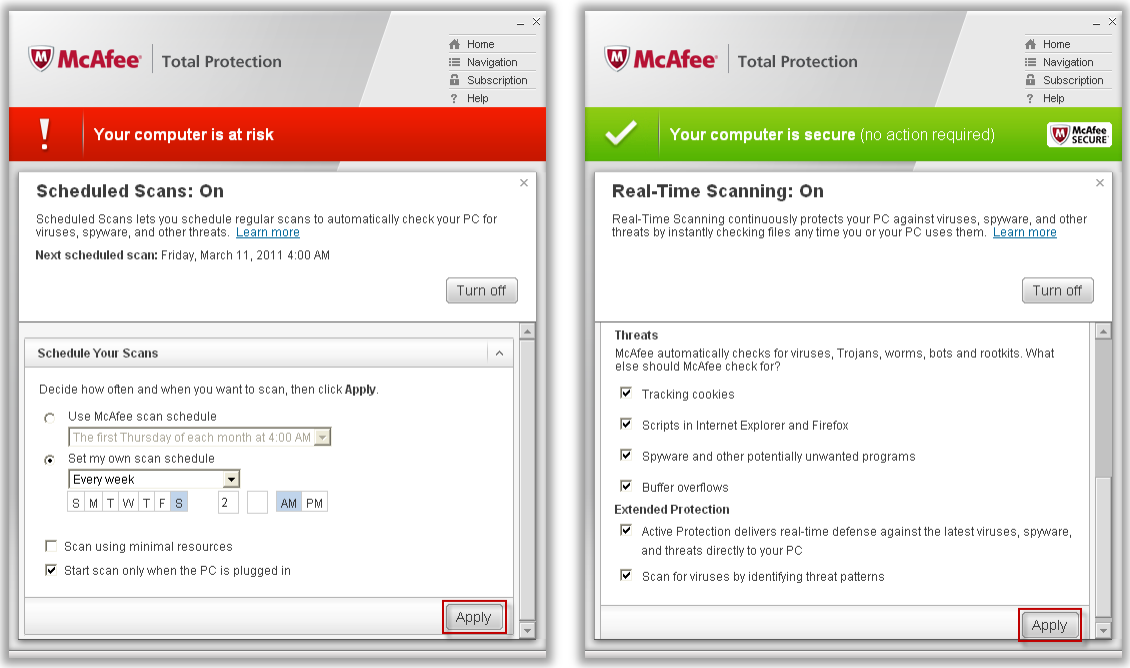

Figure 03-05: Enabling Scheduled Scan and Real-Time Scan

Configuring Kaspersky PURE

After successfully installing Kaspersky PURE, follow these steps to configure Kaspersky PURE:

Step 1: Activate the application

For Kaspersky PURE to be fully functional, it needs to be activated.

You can:

- Activate the commercial license with the purchased activation code
- Activate the trial version for 30 days and get acquainted with the possibilities of the program
- Activate later (If you select activate later, Kaspersky PURE activation will skip stage. The application will be installed on your computer, but you will be able to update the application only once after its installation.)

To continue the activation process, click **Next.**

After the license is activated, click **Next** to proceed with the configuration.

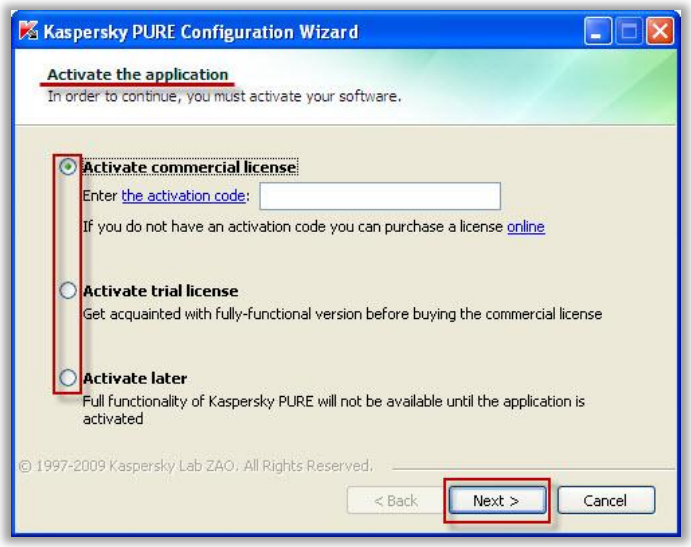

Figure 03-06: Activating the Application

Step 2: System analysis

- The Installation Wizard analyzes the system information and creates rules for trusted applications that are included in the Windows operating system. Wait until the process is complete.

Figure 03-07: System Analysis

Step 3: Completing installation

When the installation is complete, in the **The installation is complete** window:

- Make sure the box **Start Kaspersky PURE** is checked if you want to run the application immediately after the Configuration Wizard is closed.
- Clear the **Start Kaspersky PURE** box if you want to run the program later.
- To close the Configuration Wizard, click the **Finish** button.

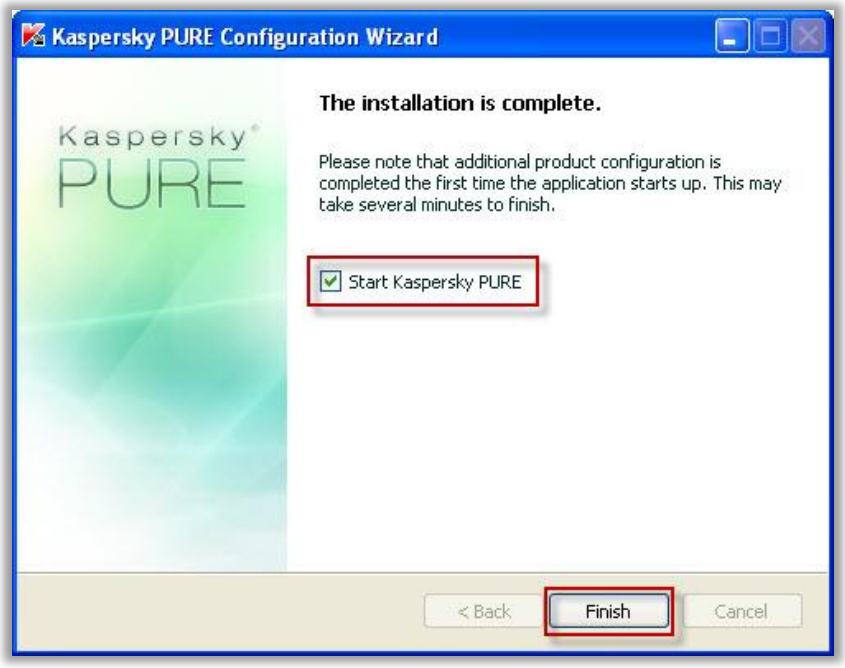

Figure 03-08: Configuring Kaspersky PURE Screenshots

Configuring Kaspersky PURE: Computer Protection

Computer Protection is a data protection tool. Components of it protect your computer against various threats, spam, and network attacks; scan all system objects for viruses and vulnerabilities; and regularly update Kaspersky PURE antivirus databases and program modules. The Computer Protection module is accessible from the Kaspersky PURE main application window.

The **Computer Protection** module includes the following protection tools:

- **Protection components:**
  - File antivirus
  - Mail antivirus
  - Web antivirus
  - IM antivirus
  - Application control
  - Firewall
  - Proactive defense
  - Network attack blocker
  - Anti-spam
  - Anti-banner
- **Virus scan tasks** are used to scan individual files, folders, drives, areas, or the entire computer for viruses
- **My Update Center** ensures that the internal application modules and databases used to scan for malicious programs are up to date

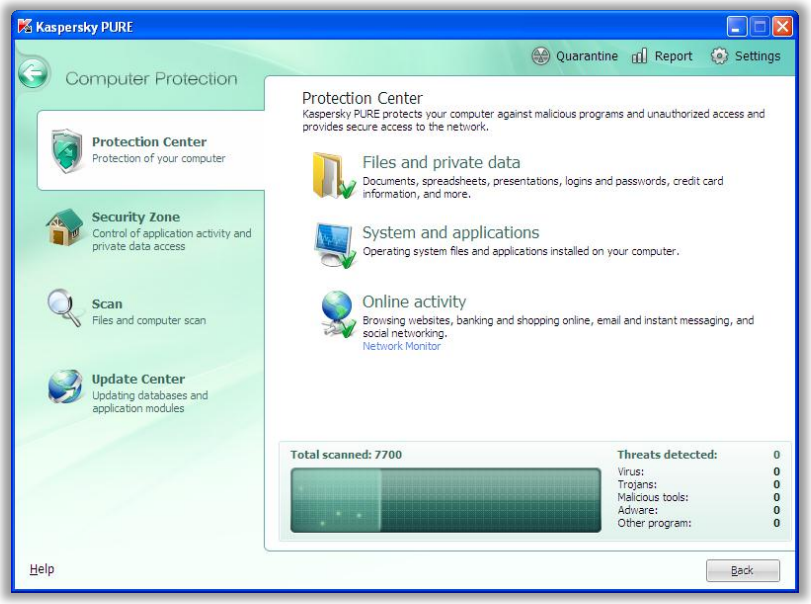

Figure 03-09: Configuring Kaspersky PURE: Computer Protection Screenshot

Configuring Kaspersky PURE: Parental Control

Kaspersky parental control is not enabled by default**.** To **protect children** and teenagers from threats related to computer and Internet usage, you should configure the Parental Control settings for all users. If you did not enable password protection when installing the application at the start-up of Parental Control, then it is recommended to **set a password** to protect against the **unauthorized modification** of control settings. Now, you can enable Parental Control and impose restrictions on computer and Internet usage as well as on instant messaging for all accounts on the computer

To ensure a reduced risk, the parental control module uses the following features:

- Restricting computer and Internet access time
- Creating lists of websites that are **allowed** and **blocked** as well as selecting categories of websites not recommended for viewing
- Enabling **safe search** mode
- Limiting files downloaded from the Internet
- Creating lists of contacts that are allowed or blocked for intercourse
- Viewing messaging text
- Forbidding certain personal data transfer
- Searching for key words in messaging texts (the number of keywords found is displayed in the Reports section)
- Creating lists of applications that are allowed and blocked for launch as well as timely restrictions for running allowed applications

Perform the following actions to configure parental control for a specific account:

- Open the main application window of **Kaspersky PURE.**
- Click the **Parental Control** button.
- In the parental control window on the **Users** tab, select the required user.
- Click the **Configure** button.

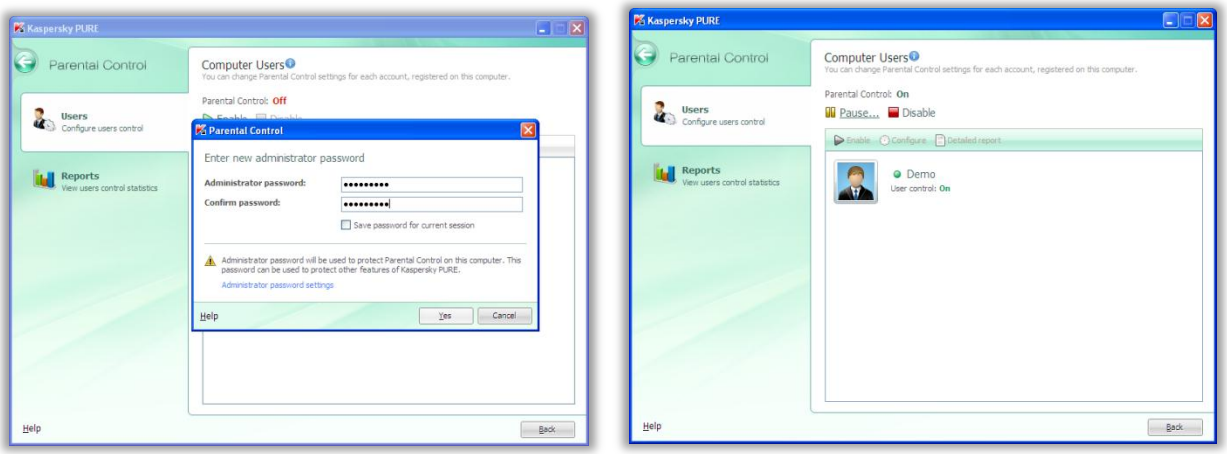

Figure 03-10: Configuring Kaspersky PURE: Parental Control Screenshots

Kaspersky PURE: Administrative Tools

Using the Administrative Tools, a user can configure the operating system and other applications to **eliminate system vulnerabilities** and ensure reliable data protection. Administrative tools enable to:

- **Tune browser settings:**

  Analyze Microsoft Internet Explorer settings by evaluating them in terms of security

- **Search for problems:**

  Search for problems related to malware activity using the Microsoft Windows Settings Troubleshooting option and delete traces left by malicious objects in the system

- **Permanently delete data:**

  Prevent unauthorized restoration of deleted files

- **Delete some unused data:**

  Delete unused and temporary files that require a considerable volume on disk space or is at risk of malware

- **Create a Rescue Disk to clean the system after a virus attack:**

  Scan and disinfects infected x86-compatible computers (used when it is impossible to disinfect the computer with the use of malware removal utilities or antivirus applications)

- **Erase user activity to protect the privacy:**

  Find and erase traces of a user's activity that enable gathering information about user activities in the system and operating system settings,

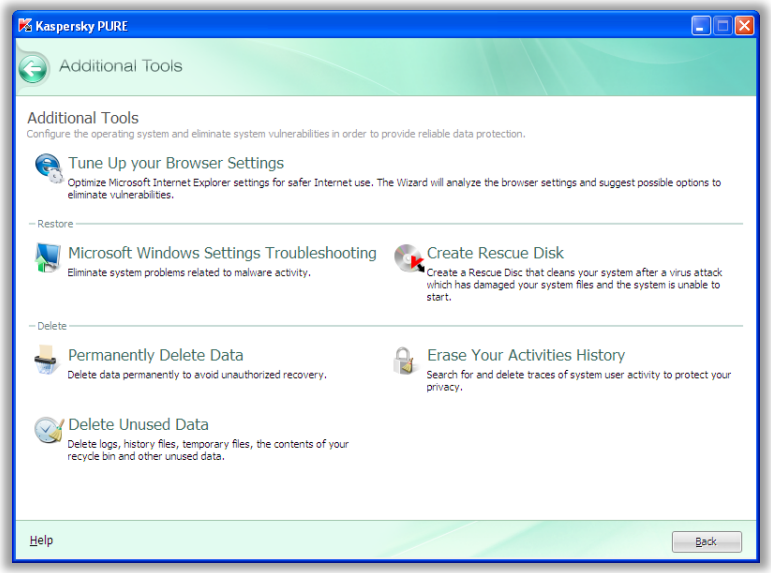

Figure 03-11: Kaspersky PURE: Administrative Tools Screenshot

Module Summary

An antivirus program protects the computer against viruses, worms, spywares, and Trojans.

A computer connected to the Internet is always at high risk, and it is always recommended to install the system with antivirus software.

Most commercial antivirus software use two techniques:

- Using virus dictionary to look for known viruses while examining files
- Detecting suspicious behavior from any computer program

In the virus dictionary approach, while examining the files, the antivirus software refers to the dictionary of known viruses identified by the author of the antivirus software.

Whenever a program with suspicious behavior is found, the antivirus software alerts the user and asks what to do.

Antivirus Security Checklist

- ☐ Do not use two antivirus programs on your computer simultaneously.
- ☐ Regularly update antivirus software and anti-spyware programs to get maximum efficiency.
- ☐ Subscribe to automatic antivirus and anti-spyware software updates whenever offered.
- ☐ Always visit the vendor's website to download the patches.
- ☐ Be cautious of free offers such as such as games, videos, music, etc.
- ☐ Be cautious while opening attachments or any links mentioned in emails.
- ☐ Uninstall software that is not in use.
- ☐ Enable real-time scanning.
- ☐ Do not open files that you are not expecting on the hard drive.
- ☐ Always perform link and email scanning.
- ☐ Enable firewall.
- ☐ Always schedule scanning.
- ☐ Use flash drives cautiously.