Acronis® Internet Security 2011

User's Guide

Acronis Internet Security 2011
User's Guide

Publication date 2010.12.06

Legal Notice

Table of Contents

Getting Started

1. Overview

Once you have installed Acronis Internet Security 2011, your computer is protected against all kinds of malware (such as viruses, spyware and trojans) and Internet threats (such as hackers, phishing and spam).

However, you may want to take advantage of the Acronis Internet Security settings to fine-tune and improve your protection. There are also some extra-features that you may find useful. Start by setting up a usage profile as presented in "*Setting Up Acronis Internet Security 2011*" (p. 6).

From time to time, you should open Acronis Internet Security and fix the existing issues. You may have to configure specific Acronis Internet Security components or take preventive actions to protect your computer and your data. If you want to, you can configure Acronis Internet Security not to alert you about specific issues. For detailed information, please refer to "*Fixing Issues*" (p. 24).

1.1. Opening Acronis Internet Security

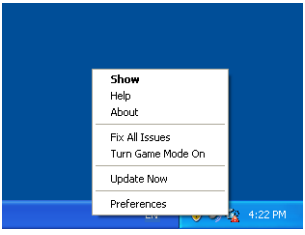
To access the main interface of Acronis Internet Security 2011, use the Windows Start menu, by following the path **Start → All Programs → Acronis Backup and Security 2011 → Acronis Internet Security 2011 → Acronis Internet Security 2011** or, quicker, double-click the Acronis Internet Security icon in the system tray.

For more information on the main application window, please refer to "*Main Application Window*" (p. 8).

1.2. System Tray Icon

To manage the entire product more quickly, you can use the Acronis Internet Security icon in the system tray. If you double-click this icon, Acronis Internet Security will open. Also, by right-clicking the icon, a contextual menu will allow you to quickly manage the Acronis Internet Security product.

- **Show** - opens the main interface of Acronis Internet Security.
- **Help** - opens the help file, which explains in detail how to configure and use Acronis Internet Security 2011.
- **About** - opens a window where you can see information about Acronis Internet Security and where to look for help in case something unexpected appears.



Tray Icon

- **Fix All Issues** - helps you remove current security vulnerabilities. If the option is unavailable, there are no issues to be fixed. For detailed information, please refer to "*Fixing Issues*" (p. 24).
- **Turn Game Mode On / Off** - activates / deactivates Game Mode.
- **Update Now** - starts an immediate update. A new window will appear where you can see the update status.
- **Preferences** - opens a window where you can enable or disable the main product settings and reconfigure your user profile. For more information, please refer to "*Configuring Main Settings*" (p. 27).

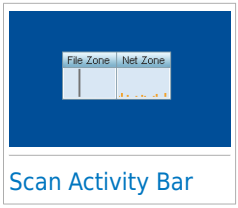
The Acronis Internet Security system tray icon informs you when issues affect your computer or how the product operates, by displaying a special symbol, as follows:

Red triangle with an exclamation mark: Critical issues affect the security of your system. They require your immediate attention and must be fixed as soon as possible.
Letter G: The product operates in Game Mode.

If Acronis Internet Security is not working, the system tray icon is grayed out . This usually happens when the license key expires. It can also occur when the Acronis Internet Security services are not responding or when other errors affect the normal operation of Acronis Internet Security.

1.3. Scan Activity Bar

The **Scan activity bar** is a graphic visualization of the scanning activity on your system. This small window is by default available only in Expert View.



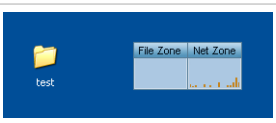
Scan Activity Bar

The gray bars (the **File Zone**) show the number of scanned files per second, on a scale from 0 to 50. The orange bars displayed in the **Net Zone** show the number of Kbytes transferred (sent and received from the Internet) every second, on a scale from 0 to 100.

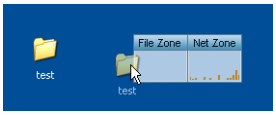
Note
The Scan activity bar will notify you when real-time protection or the Firewall is disabled by displaying a red cross over the corresponding area (**File Zone** or **Net Zone**).

1.3.1. Scan Files and Folders

You can use the Scan activity bar to quickly scan files and folders. Drag the file or folder you want to be scanned and drop it over the **Scan Activity Bar** as shown below.



Drag File



Drop File

The Antivirus Scan wizard will appear and guide you through the scanning process.

Scanning options. The scanning options are pre-configured for the best detection results. If infected files are detected, Acronis Internet Security will try to disinfect them (remove the malware code). If disinfection fails, the Antivirus Scan wizard will allow you to specify other actions to be taken on infected files. The scanning options are standard and you cannot change them.

1.3.2. Disable/Restore Scan Activity Bar

When you no longer want to see the graphic visualization, just right-click it and select **Hide**. To restore the Scan activity bar, follow these steps:

1. Open Acronis Internet Security.
2. Click the **Options** button in the upper-right corner of the window and select **Preferences**.
3. In the General Settings category, use the switch corresponding to **Scan Activity Bar** to enable it.
4. Click **OK** to save and apply the changes.

1.4. Automatic Device Detection

Acronis Internet Security automatically detects when you connect a removable storage device to your computer and offers to scan it before you access its files.

This is recommended in order to prevent viruses and other malware from infecting your computer.

Detected devices fall into one of these categories:

- CDs/DVDs
- USB storage devices, such as flash pens and external hard-drives
- mapped (remote) network drives

When such a device is detected, an alert window is displayed.

To scan the storage device, just click **Yes**. The Antivirus Scan wizard will appear and guide you through the scanning process.

If you do not want to scan the device, you must click **No**. In this case, you may find one of these options useful:

- **Don't ask me again about this type of device** - Acronis Internet Security will no longer offer to scan storage devices of this type when they are connected to your computer.
- **Disable automatic device detection** - You will no longer be prompted to scan new storage devices when they are connected to the computer.

If you accidentally disabled automatic device detection and you want to enable it, or if you want to configure its settings, follow these steps:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus>Virus Scan**.
3. In the list of scan tasks, locate the **Device Scanning** task.
4. Right-click the task and select **Properties**. A new window will appear.
5. On the **Overview** tab, configure the scanning options as needed. For more information, please refer to "*Configuring Scan Settings*" (p. 52).
6. On the **Detection** tab, choose which types of storage devices to be detected.
7. Click **OK** to save and apply the changes.

2. Setting Up Acronis Internet Security 2011

Acronis Internet Security 2011 allows you to easily configure its main settings and user interface by setting up a usage profile. The usage profile reflects the main activities performed on the computer. Depending on the usage profile, the product interface is organized to allow easy access to your preferred tasks.

After installation, a default usage profile is applied.

To reconfigure the usage profile, follow these steps:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Preferences**.
2. Click the **Reconfigure Profile** link.
3. Follow the configuration wizard. You can navigate through the wizard using the **Next** and **Back** buttons. To exit the wizard, click **Cancel**.

   a. **Choose Your View**

   Select the preferred user interface view.

   b. **Configure My Tools**

   If you have selected Basic View or Intermediate View, choose the features you would like to create shortcuts to on the Dashboard.

   c. **Configure Settings**

   If you have selected Expert View, configure the Acronis Internet Security settings as needed. To turn on or off a setting, use the corresponding switch.

   d. **Set Up Parental Control**

   Note
   This step appears only if you have added Parental Control to My Tools.

   You can select one of three options:

   - **Set Parental Control on children accounts**

     Select this option to enable Parental Control on the Windows accounts created for your children and manage it from the administrative account.

   - **Set Parental Control on current account**

     Select this option to enable Parental Control on the current Windows account. This means you will not have to create separate accounts for your children, but Parental Control rules will affect everyone using the current account.

In this case, a password is required to protect the Parental Control settings. You can set it now or at a later time from the Acronis Internet Security window.

- **Skip setup for now**

  Select this option to configure this feature at a later time from the Acronis Internet Security window.

e. **Home Network Management**

Note

This step appears only if you have added Home Network Management to My Tools.

You can select one of three options:

- **Set up this PC as "Server"**

  Select this option if you intend to manage Acronis Internet Security products on other computers in the home network from this one.

  A password is required to join the network. Enter the password in the provided text boxes and click **Submit**.

- **Set up this PC as "Client"**

  Select this option if Acronis Internet Security will be managed from another computer in the home network which is also running Acronis Internet Security.

  A password is required to join the network. Enter the password in the provided text boxes and click**Submit**.

- **Skip setup for now**

  Select this option to configure this feature at a later time from the Acronis Internet Security window.

f. **Setup Complete**

Click **Finish**.

3. Main Application Window

Acronis Internet Security 2011 meets the needs of computer beginners and very technical people alike. Its graphical user interface is designed to suit each and every category of users.

You can choose to view the user interface under any of three modes, depending on your computer skills and on your previous experience with Acronis Internet Security.

Basic View
: Suited for computer beginners and people who want Acronis Internet Security to protect their computer and data without being bothered. This mode is simple to use and requires minimal interaction on your side.

  All you have to do is fix the existing issues when indicated by Acronis Internet Security. An intuitive step-by-step wizard assists you in fixing issues. Additionally, you can perform common tasks, such as updating the Acronis Internet Security virus signature and product files or scanning the computer.

Intermediate View
: Aimed at users with average computer skills, this interface extends what you can do in Basic View.

  You can fix issues separately and choose which issues to be monitored. Moreover, you can manage remotely the Acronis Internet Security products installed on the computers in your household.

Expert View
: Suited for more technical users, this mode allows you to fully configure each functionality of Acronis Internet Security. You can also use all tasks provided to protect your computer and data.

To change the view mode:

1. Open Acronis Internet Security.
2. Click the **Options** button in the upper-right corner of the window.
3. Select the desired view mode from the menu.

3.1. Basic View

If you are a computer beginner, displaying the user interface in Basic View may be the most adequate choice for you. This mode is simple to use and requires minimal interaction on your side.

The window is organized into three main areas:

Status area
: Status information is presented in the left side of the window.

Protect Your PC area
This is where you can take the necessary actions to manage your protection.

Help area
This is where you can find out how to use Acronis Internet Security 2011 and get help.

The **Options** button in the upper-right corner of the window allows you to change the user interface view mode and to configure the main program settings.

In the bottom-right corner of the window, you can find several useful links.

Link	Description
View Logs	Allows you to see a detailed history of all tasks performed by Acronis Internet Security on your system.
Help and Support	Click this link if you need help with Acronis Internet Security.
?	Gives you access to a help file that shows you how to use Acronis Internet Security.

3.1.1. Status Area

Status information is presented in the left side of the window.

- **Security Status** informs you of the issues that affect your computer's security and helps you fix them. By clicking **Fix All Issues**, a wizard will help you easily remove any threats to your computer and data security. For detailed information, please refer to "*Fixing Issues*" (p. 24).
- **License Status** displays how many days are left until the license expires. If you are using a trial version or if your license is going to expire, you can click **Buy Now** to buy a license key.

3.1.2. Protect Your PC Area

This is where you can take the necessary actions to manage your protection.

Three buttons are available:

- **Security** provides you with shortcuts to security tasks and settings.
- **Update Now** helps you update the virus signature and product files of Acronis Internet Security. A new window will appear where you can see the update status. If updates are detected, they are automatically downloaded and installed on your computer.
- **My Tools** allows you to create shortcuts to your favorite tasks and settings.

To perform a task or configure settings, click the corresponding button and choose the desired tool from the menu. To add or remove shortcuts, click the corresponding

button and choose **More Options**. For detailed information, please refer to "*My Tools*" (p. 16).

3.1.3. Help Area

This is where you can find out how to use Acronis Internet Security 2011 and get help.

Smart Tips are a fun and easy way to learn about computer security best practices and how to use Acronis Internet Security 2011.

If you need help, type a keyword or a question in the **Help and Support** field and click **Search**.

3.2. Intermediate View

Aimed at users with average computer skills, Intermediate View is a simple interface that gives you access to all modules at a basic level. You'll have to keep track of warnings and critical alerts and fix undesired issues.

The Intermediate View window is organized into several tabs.

Dashboard
: The dashboard helps you easily monitor and manage your protection.

Security
: Displays the status of the security settings and helps you fix detected issues. You can run security tasks or configure security settings.

File Storage
: Displays the status of File Encryption and allows you to manage your file vaults.

Network
: Displays the Acronis Internet Security home network structure. This is where you can perform various actions to configure and manage the Acronis Internet Security products installed in your home network. In this way, you can manage the security of your home network from a single computer.

The **Options** button in the upper-right corner of the window allows you to change the user interface view mode and to configure the main program settings.

In the bottom-right corner of the window, you can find several useful links.

Link	Description
View Logs	Allows you to see a detailed history of all tasks performed by Acronis Internet Security on your system.
Buy/Renew	Helps you purchase a license key for your Acronis Internet Security 2011 product.

Link	Description
Help and Support	Click this link if you need help with Acronis Internet Security.
	Gives you access to a help file that shows you how to use Acronis Internet Security.

3.2.1. Dashboard

The dashboard helps you easily monitor and manage your protection.

The dashboard consists of the following sections:

- **Status Details** indicates the status of each main module using explicit sentences and one of the following icons:

  Green circle with a check mark: No issues affect the security status. Your computer and data are protected.

  Red circle with an exclamation mark: There are issues that affect the security of your system. Critical issues require your immediate attention. Non-critical issues should also be addressed as soon as possible.

  Gray circle with an exclamation mark: The activity of this module's components is not monitored. Thus, no information is available regarding their security status. There may be specific issues related to this module.

  Click the name of a module to see more details about its status and to configure status tracking for its components.

- **License Status** displays how many days are left until the license expires. If you are using a trial version or if your license is going to expire, you can click **Buy Now** to buy a license key.

- **My Tools** allows you to create shortcuts to your favorite tasks and settings. For detailed information, please refer to "*My Tools*" (p. 16).

- **Smart Tips** are a fun and easy way to learn about computer security best practices and how to use Acronis Internet Security 2011.

3.2.2. Security

The Security tab allows you to manage the security of your computer and data.

"Status Area" (p. 11)
"Quick Tasks" (p. 12)

Status Area

The status area is where you can see the complete list of monitored security components and their current status. By monitoring each security module, Acronis

Internet Security will let you know not only when you configure settings that might affect your computer's security, but also when you forget to do important tasks.

The current status of a component is indicated using explicit sentences and one of the following icons:

Green circle with a check mark: No issues affect the component.
Red circle with an exclamation mark: Issues affect the component.

Just click the **Fix** button corresponding to a sentence to fix the reported issue. If an issue is not fixed on the spot, follow the wizard to fix it.

To configure which components must be monitored:

1. Click **Add/Edit List**.
2. To turn on or off monitoring for a specific item, use the corresponding switch.
3. Click **Close** to save the changes and close the window.

Important
To ensure that your system is fully protected, enable tracking for all components and fix all reported issues.

Quick Tasks

This is where you can find links to the most important security tasks:

- **Update Now** - starts an immediate update.
- **Full System Scan** - starts a standard scan of your computer (archives excluded). For additional on-demand scan tasks, click the arrow on this button and select a different scan task.
- **Custom Scan** - starts a wizard that lets you create and run a custom scan task.
- **Vulnerability Scan** - starts a wizard that checks your system for vulnerabilities and helps you fix them.
- **Parental Control** - opens the Parental Control configuration window. For more information, please refer to "*Parental Control*" (p. 77).
- **Configure Firewall** - opens a window where you can view and configure the Firewall settings. For more information, please refer to "*Firewall*" (p. 97).

3.2.3. File Storage

In the File Storage tab, you can store your sensitive files in encrypted file vaults to prevent them from being accessed by someone else.

"Status Area" (p. 13)
"Quick Tasks" (p. 13)

Status Area

The current status of a component is indicated using explicit sentences and one of the following icons:

Green circle with a check mark: No issues affect the component.
Red circle with an exclamation mark: Issues affect the component.

Just click the **Fix** button corresponding to a sentence to fix the reported issue.

To configure which components must be monitored:

1. Click **Add/Edit List**.
2. To turn on or off monitoring for a specific item, use the corresponding switch.
3. Click **Close** to save the changes and close the window.

Quick Tasks

The following buttons are available:

- **Add File to Vault** - starts the wizard that allows you to store your important files / documents privately by encrypting them in special, vaulted drives.
- **Remove Vault Files** - starts the wizard that allows you to erase data from the file vault.
- **View File Vault** - starts the wizard that allows you to view the content of your file vaults.
- **Lock File Vault** - starts the wizard that allows you to lock your vault in order to start protecting its content.

For detailed information on how to protect your files using file vaults, please refer to "*File Encryption*" (p. 114).

3.2.4. Network

This is where you can perform various actions to configure and manage the Acronis Internet Security products installed in your home network. In this way, you can manage the security of your home network from a single computer.

For detailed information, please refer to "*Home Network*" (p. 131).

3.3. Expert View

Expert View gives you access to each specific component of Acronis Internet Security. This is where you can configure Acronis Internet Security in detail.

Note
Expert View is suited for users having above average computer skills, who know the type of threats a computer is exposed to and how security programs work.

On the left side of the window there is a menu containing all security modules. Each module has one or more tabs where you can configure the corresponding security settings or perform security or administrative tasks. The following list briefly describes each module. For detailed information, please refer to the "Configuration and Management" (p. 33) part of this user guide.

General
: Allows you to access the general settings or to view the dashboard and detailed system info.

Antivirus
: Allows you to configure your virus shield and scanning operations in detail, to set exceptions and to configure the quarantine module. This is were you can also configure antiphishing protection and Search Advisor.

Antispam
: Allows you to keep your Inbox SPAM-free and to configure the antispam settings in detail.

Parental Control
: Allows you to protect your children against inappropriate content by using your customized computer access rules.

Privacy Control
: Allows you to prevent data theft from your computer and protect your privacy while you are online.

Firewall
: Allows you to protect your computer from inbound and outbound unauthorized connection attempts. It is quite similar to a guard at your gate - it will keep a watchful eye on your Internet connection and keep track of who to allow access to the Internet and who to block.

Vulnerability
: Allows you to keep crucial software on your PC up-to-date.

Encryption
: Allows you to encrypt Yahoo and Windows Live (MSN) Messenger communications and also to local encrypt your critical files, folders or partitions.

Game/Laptop Mode
: Allows you to postpone the Acronis Internet Security scheduled tasks while your laptop runs on batteries and also to eliminate all alerts and pop-ups when you are playing.

Home Network
: Allows you to configure and manage several computers in your household.

Update
: Allows you to obtain info on the latest updates, to update the product and to configure the update process in detail.

Registration
Allows you to register your product with a new license key.

The **Options** button in the upper-right corner of the window allows you to change the user interface view mode and to configure the main program settings.

In the bottom-right corner of the window, you can find several useful links.

Link	Description
View Logs	Allows you to see a detailed history of all tasks performed by Acronis Internet Security on your system.
Buy/Renew	Helps you purchase a license key for your Acronis Internet Security 2011 product.
Help and Support	Click this link if you need help with Acronis Internet Security.
	Gives you access to a help file that shows you how to use Acronis Internet Security.

4. My Tools

When using Acronis Internet Security in Basic View or Intermediate View, you can customize your dashboard by adding shortcuts to tasks and settings that are important to you. This way, you can quickly gain access to features you use regularly and to advanced settings without having to switch to a more advanced interface view mode.

Depending on the user interface view mode you use, the shortcuts added to My Tools are available as follows:

Basic View
: In the Protect Your PC area, click **My Tools**. A menu will appear. Click a shortcut to launch the corresponding tool.

Intermediate View
: The shortcuts appear under My Tools. Click a shortcut to launch the corresponding tool.

To open the window from which you can select the shortcuts that will appear in My Tools, proceed as follows:

Basic View
: In the Protect Your PC area, click My Tools and choose **More Options**.

Intermediate View
: Click one of the buttons under My Tools or the **Configure** link.

Use the switches to select the tools to be added to My Tools. You can select any of the following categories of tools.

- **Scan Tasks**

  Add the tasks you regularly use to scan your system for security threats.

Scan Task	Description
Full System Scan	Scans the entire system, except for archives. In the default configuration, it scans for all types of malware other than rootkits.
My Documents Scan	Use this task to scan important current user folders: `My Documents`, `Desktop` and `StartUp`. This will ensure the safety of your documents, a safe workspace and clean applications running at startup.
Custom Scan	Starts a wizard that lets you create a custom scan task.
Deep System Scan	Scans the entire system. In the default configuration, it scans for all types of malware threatening your

Scan Task	Description
	system's security, such as viruses, spyware, adware, rootkits and others.
Quick Scan	Quick Scan uses in-the-cloud scanning to detect malware running in your system. Running a Quick Scan usually takes less than a minute and uses a fraction of the system resources needed by a regular virus scan.
Schedule My Scans	Takes you to the Antivirus settings window where you can customize the on-demand scan tasks.

For more information about scan tasks, please refer to "*Managing Existing Scan Tasks*" (p. 49).

- **Settings**

  Add shortcuts to the Acronis Internet Security settings you want to configure:

Settings	Description
Update Now	Trigger an update of Acronis Internet Security. For more information, please refer to "*Update*" (p. 135).
Parental Control	Configure the Parental Control module. For more information, please refer to "*Parental Control*" (p. 77).
Configure Firewall	Configure the Firewall module. For more information, please refer to "*Firewall*" (p. 97).
Game Mode	Toggle the Game Mode. For more information, please refer to "*Game Mode*" (p. 125).
Laptop Mode	Toggle the Laptop Mode. For more information, please refer to "*Laptop Mode*" (p. 128).
Configure Antivirus	Configure the Antivirus module. For more information, please refer to "*Antivirus Protection*" (p. 38).
View & Fix All Issues	Open a wizard that will help you fix all the security issues affecting your system. For more information, please refer to "*Fixing Issues*" (p. 24).

- **Help & Support**

  Allows you to contact the Acronis support team.

5. Alerts and Pop-ups

Acronis Internet Security uses pop-ups and alerts to inform you about its operation or special events that may interest you and to prompt you for action when needed. This chapter presents the Acronis Internet Security pop-ups and alerts that you may encounter.

Pop-ups are small windows that temporarily appear on the screen to inform you about various Acronis Internet Security events, such as e-mail scanning, a new computer that logged to your wireless network, a firewall rule added etc. When pop-ups appear, you will be required to click an **OK** button or a link, at the most.

Alerts are larger windows that prompt you for action or inform you about something very important (for example, a virus has been detected). Besides alert windows, you may receive e-mail, instant message or web page alerts.

The Acronis Internet Security pop-ups and alerts include:

- Antivirus Alerts
- Active Virus Control Alerts
- Device Detection Alerts
- Firewall Pop-ups and Alerts
- Antiphishing Alert Web Pages
- Parental Control Alert Messages
- Privacy Control Alerts

5.1. Antivirus Alerts

Acronis Internet Security protects you against various kinds of malware, such as viruses, spyware or rootkits. When it detects a virus or other malware, Acronis Internet Security takes a specific action on the infected file and informs you about it through an alert window.

You can see the virus name, the path to the infected file and the action taken by Acronis Internet Security.

Click **OK** to close the window.

Important

When a virus is detected, it is best practice to scan the entire computer to make sure there are no other viruses. For more information, please refer to "*How Do I Scan Files and Folders?*" (p. 140).
If the virus has not been blocked, please refer to "*Removing Malware from Your System*" (p. 164).

5.2. Active Virus Control Alerts

Active Virus Control can be configured to alert you and prompt you for action whenever an application tries to perform a possible malicious action.

If you are using the Basic View or Intermediate View interface, a pop-up will inform you whenever Active Virus Control blocks a potentially harmful application. If you are using Expert View, you will be prompted for action, through an alert window, when an application exhibits malicious behavior.

If you know and trust the detected application, click **Allow**.

If you want to immediately close the application, click **OK**.

Select the **Remember this action for this application** check box before making your choice and Acronis Internet Security will take the same action for the detected application in the future. The rule that is thus created will be listed in the Active Virus Control configuration window.

5.3. Device Detection Alerts

Acronis Internet Security automatically detects when you connect a removable storage device to your computer and offers to scan it before you access its files. This is recommended in order to prevent viruses and other malware from infecting your computer.

Detected devices fall into one of these categories:

- CDs/DVDs
- USB storage devices, such as flash pens and external hard-drives
- mapped (remote) network drives

When such a device is detected, an alert window is displayed.

To scan the storage device, just click **Yes**. The Antivirus Scan wizard will appear and guide you through the scanning process.

If you do not want to scan the device, you must click **No**. In this case, you may find one of these options useful:

- **Don't ask me again about this type of device** - Acronis Internet Security will no longer offer to scan storage devices of this type when they are connected to your computer.
- **Disable automatic device detection** - You will no longer be prompted to scan new storage devices when they are connected to the computer.

If you accidentally disabled automatic device detection and you want to enable it, or if you want to configure its settings, follow these steps:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.

2. Go to **Antivirus>Virus Scan**.
3. In the list of scan tasks, locate the **Device Scanning** task.
4. Right-click the task and select **Properties**. A new window will appear.
5. On the **Overview** tab, configure the scanning options as needed. For more information, please refer to "*Configuring Scan Settings*" (p. 52).
6. On the **Detection** tab, choose which types of storage devices to be detected.
7. Click **OK** to save and apply the changes.

5.4. Firewall Pop-ups and Alerts

The firewall uses pop-ups to inform you about various events related to your network connection (for example, when a new computer connects to your Wi-Fi network, when a new application is allowed to access the Internet or when a port scan is blocked). These pop-ups may be very useful in detecting intrusion attempts and protecting yourself against network threats.

If you are using Expert View, you will be prompted for action, through an alert window, whenever an unknown application tries to connect to the Internet.

You can see the following: the application that is trying to access the Internet, the path to the application file, the destination, the protocol used and the port on which the application is trying to connect.

Click **Allow** to allow all traffic (inbound and outbound) generated by this application from the local host to any destination, over the respective IP protocol and on all ports. If you click **Block**, the application will be denied access to the Internet over the respective IP protocol completely.

Important
Allow inbound connection attempts only from IPs or domains you are sure to trust.

Based on your answer, a rule will be created, applied and listed in the table. The next time the application tries to connect, this rule will be applied by default.

If you are using Basic View or Intermediate View, the connection attempt will be automatically blocked.

5.5. Antiphishing Alerts

With antiphishing protection enabled, Acronis Internet Security alerts you when you try to access web pages that may be set up to steal personal information. Before you can access such a web page, Acronis Internet Security will block that page and display a generic web page alert instead.

Check the web page address in the address bar of your browser. Look for clues that might indicate that the web page is used for phishing. If the web address is suspicious, it is recommended that you do not open it.

Here are some tips you may find useful:

- If you have typed the address of a legitimate website, check if the address is correct. If the address is incorrect, re-type it and go to the web page again.
- If you have clicked a link in an e-mail or an instant message, verify who sent it to you. If the sender is unknown, this is probably a phishing attempt. If you know the sender, you should check if that person really sent you the link.
- If you reached the web page by browsing the Internet, check the web page where you found the link (click the Back button on your web browser).

If you want to view the web page, click the appropriate link to take one of these actions:

- **View the web page this time only.** There is no risk as long as you do not submit any information on the web page. If the web page is legitimate, you can add it to the White List (click the Acronis Internet Security Antiphishing toolbar and select **Add to White List**).
- **Add the web page to the White List.** The web page will be displayed immediately and Acronis Internet Security will no longer alert you about it.

Important

Add to the White List only the web pages that you fully trust (for example, your bank's web address, known online shops, etc). Acronis Internet Security does not check for phishing the web pages in the White List.

You can manage antiphishing protection and the White List using the Acronis Internet Security toolbar in your web browser. For more information, please refer to *"Managing the Acronis Internet Security Antiphishing Protection in Internet Explorer and Firefox"* (p. 61).

5.6. Parental Control Alert Messages

You can configure Parental Control to block:

- inappropriate web pages.
- Internet access, for specific periods of time (such as when it's time for lessons).
- web pages, e-mail messages and instant messages if they contain specific keywords.
- applications like games, chat, filesharing programs or others.
- instant messages sent by IM contacts other than those allowed.

The user is informed whenever an activity is blocked through a specific alert message (for example, a standard alert web page, e-mail or instant message). Detailed information is provided so that the user can find out why the activity was blocked.

5.7. Privacy Control Alerts

Privacy Control provides advanced users with some extra features to protect their privacy. You will be prompted for action through specific alert windows if you choose to enable any of these components:

- Registry Control - asks for your permission whenever a program tries to modify a registry entry in order to be executed at Windows start-up.
- Cookie Control - asks for your permission whenever a new website tries to set a cookie.
- Script Control - asks for your permission whenever a website tries to activate a script or other active content.

5.7.1. Registry Alerts

If you enable Registry Control, you will be prompted for permission whenever a new program tries to modify a registry entry in order to be executed at Windows start-up.

You can see the program that is trying to modify Windows Registry.

Note
Acronis Internet Security will usually alert you when you install new programs that need to run after the next startup of your computer. In most cases, these programs are legitimate and can be trusted.

If you do not recognize the program and if it seems suspicious, click **Block** to prevent it from modifying Windows Registry. Otherwise, click **Allow** to permit the modification.

Based on your answer, a rule is created and listed in the rules table. The same action is applied whenever this program tries to modify a registry entry.

For more information, please refer to "*Registry Control*" (p. 93).

5.7.2. Script Alerts

If you enable Script Control, you will be prompted for permission whenever a new web site tries to run a script or other active content.

You can see the name of the resource.

Click **Yes** or **No** and a rule will be created, applied and listed in the rules table. The same action will be applied automatically whenever the respective site tries to run active content.

Note
Some web pages may not be properly displayed if you block active content.

For more information, please refer to "*Script Control*" (p. 95).

5.7.3. Cookie Alerts

If you enable Cookie Control, you will be prompted for permission whenever a new web site tries to set or request a cookie.

You can see the name of the application that is trying to send the cookie file.

Click **Yes** or **No** and a rule will be created, applied and listed in the rules table. The same action will be applied automatically whenever you connect to the respective site.

For more information, please refer to "*Cookie Control*" (p. 93).

6. Fixing Issues

Acronis Internet Security uses an issue tracking system to detect and inform you about the issues that may affect the security of your computer and data. By default, it will monitor only a series of issues that are considered to be very important. However, you can configure it as needed, choosing which specific issues you want to be notified about.

This is how pending issues are notified:

- A special symbol is displayed over the Acronis Internet Security icon in the system tray to indicate pending issues. Also, if you move the mouse cursor over the icon, a pop-up will confirm the existence of pending issues.
- When you open Acronis Internet Security, the Security Status area will indicate the number of issues affecting your system.
  - ▶ In Basic View, the security status is displayed on the left side of the window.
  - ▶ In Expert View, go to **General > Dashboard** to check the security status.

6.1. Fix Issues Wizard

The easiest way to fix the existing issues is to follow the **Fix Issues Wizard**. To open the wizard, do any of the following:

- Right-click the Acronis Internet Security icon in the system tray and select **Fix All Issues**.
- Open Acronis Internet Security and, depending on the user interface view mode, proceed as follows:
  - ▶ In Basic View, click **View All Issues**.
  - ▶ In Expert View, go to **General > Dashboard** and click **View All Issues**.

Note
You can also add a shortcut to My Tools.

A list of existing security threats on your computer is displayed.

All current issues are selected to be fixed. If there is an issue that you do not want to be fixed, just clear the corresponding check box. If you do so, its status will change to **Skip**.

Note
If you do not want to be notified about specific issues, you must configure the alert system accordingly, as described in the next section.

To fix the selected issues, click **Start**. Some issues are fixed immediately. For others, a wizard helps you fix them.

The issues that this wizard helps you fix can be grouped into these main categories:

- **Disabled security settings.** Such issues are fixed immediately, by enabling the respective security settings.
- **Preventive security tasks you need to perform.** An example of such a task is scanning your computer. It is recommended that you scan your computer at least once a week. Acronis Internet Security will automatically do that for you in most cases. However, if you have changed the scanning schedule or if the schedule is not completed, you will be notified about this issue.

  When fixing such issues, a wizard helps you successfully complete the task.
- **System vulnerabilities.** Acronis Internet Security automatically checks your system for vulnerabilities and alerts you about them. System vulnerabilities include the following:

  ▶ weak passwords to Windows user accounts.

  ▶ outdated software on your computer.

  ▶ missing Windows updates.

  ▶ Windows Automatic Updates is disabled.

  When such issues are to be fixed, the vulnerability scan wizard is started. This wizard assists you in fixing the detected system vulnerabilities. For detailed information, please refer to section "*Checking for Vulnerabilities*" (p. 109).

6.2. Configuring Status Alerts

The status alert system is pre-configured to monitor and alert you about the most important issues that may affect the security of your computer and data. Besides the issues monitored by default, there are several other issues you can be informed about.

You can configure the alert system to best serve your security needs by choosing which specific issues to be informed about. You can do this either in Intermediate View or in Expert View.

- In Intermediate View, the alert system can be configured from separate locations. Follow these steps:
  1. Go to the **Security** tab.
  2. Click the **Add/Edit List** link in the Status area.
  3. Use the switch corresponding to an item to change its alert state.
- In Expert View, the alert system can be configured from a central location. Follow these steps:
  1. Go to **General > Dashboard**.

2. Click **Add/Edit Alerts**.
3. Use the switch corresponding to an item to change its alert state.

7. Configuring Main Settings

You can configure the main product settings (including reconfiguring the usage profile) from the Preferences window. To open it, do any of the following:

- Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Preferences**.
- Right-click the Acronis Internet Security icon in the system tray and select **Preferences**.

Note

To configure the product settings in detail, use the Expert View interface. For detailed information, please refer to the "Configuration and Management" (p. 33) part of this user guide.

The settings are organized into three categories:

- Security Settings
- Alerts Settings
- General Settings

To turn on or off a setting, use the corresponding switch.

To apply and save the configuration changes you make, click **OK**. To close the window without saving the changes, click **Cancel**.

The **Reconfigure Profile** link in the upper-right corner of the window allows you to reconfigure the usage profile. For more information, please refer to "*Setting Up Acronis Internet Security 2011*" (p. 6).

7.1. Security Settings

In this area, you can enable or disable product settings that cover various aspects of computer and data security. To turn on or off a setting, use the corresponding switch.

Warning

Use caution when disabling real-time antivirus protection, firewall or automatic update. Disabling these features may compromise your computer's security. If you really need to disable them, remember to re-enable them as soon as possible.

These are the available settings:

Antivirus

Real-time protection ensures that all files are scanned as they are accessed by you or by an application running on this system.

Automatic Update

Automatic update ensures that the newest Acronis Internet Security product and signature files are downloaded and installed automatically, on a regular basis. Updates are performed by default every hour.

Vulnerability Scan

Automatic Vulnerability Scan alerts you about and helps you fix vulnerabilities in your system that might affect its security. Such vulnerabilities include outdated software, weak passwords to user accounts or missing Windows updates.

Antispam

Antispam filters the e-mail messages that you receive, marking unsolicited and junk mail as SPAM.

Antiphishing

Antiphishing detects and alerts you in real-time if a web page is set up to steal personal information.

Search Advisor

Search Advisor scans the links in your search results and informs you which of them are safe and which are not.

Identity Control

Identity Control helps you prevent your personal data from being sent out on the Internet without your consent. It blocks any instant messages, e-mail messages or web forms transmitting data you defined as being private to unauthorized recipients (addresses).

Chat Encryption

Chat Encryption secures your conversations via Yahoo! Messenger and Windows Live Messenger provided that your IM contacts use a compatible Acronis Internet Security product and IM software.

Parental Control (current user)

Parental Control restricts the computer and online activities of your children based on the rules you defined. Restrictions may include blocking inappropriate web sites, as well as limiting gaming and Internet access according to a specified schedule.

Firewall

Firewall protects your computer from hacker and malicious outside attacks.

File Encryption

File Encryption keeps your documents private by encrypting them in special vaulted drives. If you disable File Encryption, all file vaults will be locked and you will no longer be able to access the files they contain.

The status of some of these settings may be monitored by the Acronis Internet Security issue tracking system. If you disable a monitored setting, Acronis Internet Security will indicate this as an issue that you need to fix.

If you do not want a monitored setting that you disabled to be shown as an issue, you must configure the tracking system accordingly. You can do that either in Intermediate View or in Expert View. For detailed information, please refer to "*Configuring Status Alerts*" (p. 25).

7.2. Alerts Settings

In this area, you can turn off the Acronis Internet Security pop-ups and alerts. Acronis Internet Security uses alerts to prompt you for action and pop-ups to inform you about actions it has taken automatically or about other events. To turn on or off a category of alerts, use the corresponding switch.

Important

Most of these alerts and pop-ups should be kept turned on in order to avoid potential problems.

These are the available settings:

Antivirus Alerts

Antivirus alerts inform you when Acronis Internet Security detects and blocks a virus. When a virus is detected, it is best practice to scan the entire computer to make sure there are no other viruses.

Active Virus Control Pop-ups

If you are using the Basic View or Intermediate View interface, a pop-up will inform you whenever Active Virus Control blocks a potentially harmful application. If you are using Expert View, you will be prompted for action, through an alert window, when an application exhibits malicious behavior.

Scan Email Pop-ups

These pop-ups are displayed to inform you that Acronis Internet Security is scanning e-mails for malware.

Home Network Management Alerts

These alerts inform the user when administrative actions are being performed remotely.

Firewall Pop-ups

The firewall uses pop-ups to inform you about various events related to your network connection (for example, when a new computer connects to your Wi-Fi network, when a new application is allowed to access the Internet or when a port scan is blocked). If you are using Expert View, you will be prompted for action, through an alert window, whenever an unknown application tries to connect to the Internet.

These pop-ups may be very useful in detecting intrusion attempts and protecting yourself against network threats.

Quarantine Alerts
Quarantine alerts inform you when old quarantined files have been deleted.

Parental Control Alerts
Whenever Parental Control blocks an activity, an alert is displayed to inform the user why the activity is being blocked (for example, an alert web page is displayed instead of a blocked web page).

Registration Pop-ups
Registration pop-ups are used to remind you that you need to register Acronis Internet Security or to inform you that the license key is about to or has already expired.

7.3. General Settings

In this area, you can enable or disable settings that affect product behavior and user experience. To turn on or off a setting, use the corresponding switch.

These are the available settings:

Game Mode
Game Mode temporarily modifies protection settings so as to minimize their impact on system performance during games.

Laptop Mode Detection
Laptop Mode temporarily modifies protection settings so as to minimize their impact on the life of your laptop battery.

Settings Password
To prevent someone else from changing the Acronis Internet Security settings, you can protect them with a password. When you enable this option, you will be prompted to configure the settings password. Type the desired password in both fields and click **OK** to set the password.

Acronis Internet Security News
By enabling this option, you will receive important company news, product updates or new security threats from Acronis Internet Security.

Product Notification Alerts
By enabling this option, you will receive information alerts.

Scan Activity Bar
The Scan Activity Bar is a small, transparent window indicating the progress of the Acronis Internet Security scanning activity.

Send Virus Reports
By enabling this option, virus scanning reports are sent to Acronis Internet Security labs for analysis. Please note that these reports will contain no

confidential data, such as your name or IP address, and that they will not be used for commercial purposes.

Outbreak Detection

By enabling this option, reports regarding potential virus-outbreaks are sent to Acronis Internet Security labs for analysis. Please note that these reports will contain no confidential data, such as your name or IP address, and that they will not be used for commercial purposes.

8. History and Events

The **View Logs** link at the bottom of the Acronis Internet Security main window opens another window with the Acronis Internet Security history & events. This window offers you an overview of the security-related events. For instance, you can easily check if the update was successfully performed, if malware was found on your computer etc.

In order to help you filter the Acronis Internet Security history & events, the following categories are provided on the left side:

- **Dashboard**
- **Antivirus**
- **Antispam**
- **Parental Control**
- **Privacy Control**
- **Firewall**
- **Vulnerability**
- **Chat encryption**
- **File encryption**
- **Game/Laptop Mode**
- **Home Network**
- **Update**
- **Registration**

A list of events is available for each category. Each event comes with the following information: a short description, the action Acronis Internet Security took on it when it happened, and the date and time when it occurred. If you want to find out more information about a particular event in the list, double-click that event.

This is also where you can view detailed information and statistics regarding Parental Control events such as websites accessed or applications used by your children.

Click **Clear all logs** if you want to remove old logs or **Refresh** to make sure the latest logs are displayed.

Configuration and Management

9. General Settings

The General module provides information on the Acronis Internet Security activity and the system. Here you can also change the overall behavior of Acronis Internet Security.

To configure the general settings:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **General > Settings**.

- **Enable password protection for product settings** - enables setting a password in order to protect the Acronis Internet Security configuration.

  Note

  If you are not the only person with administrative rights using this computer, it is recommended that you protect your Acronis Internet Security settings with a password.

  Type the password in the **Password** field, re-type it in the **Retype password** field and click **OK**.

  Once you have set the password, you will be asked for it whenever you want to change the Acronis Internet Security settings. The other system administrators (if any) will also have to provide this password in order to change the Acronis Internet Security settings.

  If you want to be prompted for the password only when configuring Parental Control, you must also select **Apply password protection to parental control settings only**. On the other hand, if a password was set only for Parental Control and you uncheck this option, the respective password will be requested when configuring any Acronis Internet Security option.

  Important

  If you forgot the password you will have to repair the product in order to modify the Acronis Internet Security configuration.

- **Ask me if I want to create a password when I enable Parental Control** - prompts you to configure a password when you want to enable Parental Control and no password is set. By setting a password, you will prevent other users with administrative rights from changing the Parental Control settings that you configured for a specific user.
- **Show Acronis Internet Security News (security related notifications)** - shows from time to time security notifications regarding virus outbreaks, sent by the Acronis Internet Security server.

- **Show pop-ups (on-screen notes)** - shows pop-up windows regarding the product status. You can configure Acronis Internet Security to display pop-ups only when the interface is in Basic / Intermediate View or in Expert View.
- **Show the Scan Activity bar (on screen graph of product activity)** - displays the Scan Activity bar whenever you log on to Windows. Clear this check box if you do not want the Scan Activity bar to be displayed anymore.

Virus Report Settings

- **Send virus reports** - sends to the Acronis Internet Security Labs reports regarding viruses identified in your computer. It helps us keep track of virus-outbreaks.

  The reports will contain no confidential data, such as your name, IP address or others, and will not be used for commercial purposes. The information supplied will contain only the virus name and will be used solely to create statistic reports.
- **Enable Acronis Internet Security Outbreak Detection** - sends to the Acronis Internet Security Labs reports regarding potential virus-outbreaks.

  The reports will contain no confidential data, such as your name, IP address or others, and will not be used for commercial purposes. The information supplied will contain only the potential virus and will be used solely to detect new viruses.

Connection Settings

Several Acronis Internet Security components (the Firewall, LiveUpdate, Real-Time Virus Reporting and Real-Time Spam Reporting modules) require access to the Internet. Acronis Internet Security comes with a proxy manager that allows configuring from one location the proxy settings used by the Acronis Internet Security components to access the Internet.

If your company uses a proxy server to connect to the Internet, you must specify the proxy settings in order for Acronis Internet Security to update itself. Otherwise, it will use the proxy settings of the administrator that installed the product or of the current user's default browser, if any. For more information, please refer to *"How Do I Find Out My Proxy Settings?"* (p. 173).

Note

The proxy settings can be configured only by users with administrative rights on the computer or by power users (users who know the password to the product settings).

To manage the proxy settings, click **Proxy Settings**.

There are three sets of proxy settings:

- **Proxy Detected at Install Time** - proxy settings detected on the administrator's account during installation and which can be configured only if you are logged

on to that account. If the proxy server requires a username and a password, you must specify them in the corresponding fields.

- **Default Browser Proxy** - proxy settings of the current user, extracted from the default browser. If the proxy server requires a username and a password, you must specify them in the corresponding fields.

  Note

  The supported web browsers are Internet Explorer, Mozilla Firefox and Opera. If you use another browser by default, Acronis Internet Security will not be able to obtain the proxy settings of the current user.

- **Custom Proxy** - proxy settings that you can configure if you are logged in as an administrator.

  The following settings must be specified:

  ▶ **Address** - type in the IP of the proxy server.
  ▶ **Port** - type in the port Acronis Internet Security uses to connect to the proxy server.
  ▶ **Username** - type in a user name recognized by the proxy.
  ▶ **Password** - type in the valid password of the previously specified user.

Acronis Internet Security will use the proxy settings sets in the following order until it manages to connect to the Internet:

1. the specified proxy settings.
2. the proxy settings detected at install time.
3. the proxy settings of the current user.

When trying to connect to the Internet, each set of proxy settings is tried at a time, until Acronis Internet Security manages to connect.

First, the set containing your own proxy settings will be used to connect to the Internet. If it does not work, the proxy settings detected at installation time will be tried next. Finally, if those do not work either, the proxy settings of the current user will be taken from the default browser and used to connect to the Internet.

Click **OK** to save the changes and close the window.

Click **Apply** to save the changes or click **Default** to load the default settings.

System Information

Acronis Internet Security allows you to view, from a single location, all system settings and the applications registered to run at startup. In this way, you can monitor the activity of the system and of the applications installed on it as well as identify possible system infections.

To obtain system information:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **General > System Info**.

The list contains all the items loaded when starting the system as well as the items loaded by different applications.

Three buttons are available:

- **Restore** - changes a current file association to default. Available for the **File Associations** settings only!
- **Go to** - opens a window where the selected item is placed (the **Registry** for example).

Note

Depending on the selected item, the **Go to** button may not appear.

- **Refresh** - re-opens the **System Info** section.

10. Antivirus Protection

Acronis Internet Security protects your computer from all kinds of malware (viruses, Trojans, spyware, rootkits and so on). The protection Acronis Internet Security offers is divided into two categories:

- Real-time protection - prevents new malware threats from entering your system. Acronis Internet Security will, for example, scan a word document for known threats when you open it, and an e-mail message when you receive one.

  Real-time protection is also referred to as on-access scanning - files are scanned as the users access them.

  Important

  To prevent viruses from infecting your computer keep **Real-time protection** enabled.

- On-demand scanning - allows detecting and removing the malware that already resides in the system. This is the classic scan initiated by the user - you choose what drive, folder or file Acronis Internet Security should scan, and Acronis Internet Security scans it - on-demand. The scan tasks allow you to create customized scanning routines and they can be scheduled to run on a regular basis.

When it detects a virus or other malware, Acronis Internet Security will automatically attempt to remove the malware code from the infected file and reconstruct the original file. This operation is referred to as disinfection. Files that cannot be disinfected are moved to quarantine in order to contain the infection. For more information, please refer to "*Quarantine Area*" (p. 58).

If your computer has been infected with malware, please refer to "*Removing Malware from Your System*" (p. 164).

Advanced users can configure scan exclusions if they do not want specific files to be scanned. For more information, please refer to "*Configuring Scan Exclusions*" (p. 55).

10.1. Real-time Protection

Acronis Internet Security provides continuous, real-time protection against a wide range of malware threats by scanning all accessed files, e-mail messages and the communications through Instant Messaging Software applications (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

The default real-time protection settings ensure good protection against malware, with minor impact on system performance. You can easily change the real-time protection settings according to your needs by switching to one of the predefined

protection levels. Or, if you are an advanced user, you can configure the scan settings in detail by creating a custom protection level.

To learn more, please refer to these topics:

- "*Adjusting the Real-time Protection Level*" (p. 39)
- "*Creating a Custom Protection Level*" (p. 39)
- "*Changing the Actions Taken on Detected Files*" (p. 41)
- "*Restoring the Default Settings*" (p. 42)

To protect you against unknown malicious applications, Acronis Internet Security uses an advanced heuristic technology (Active Virus Control) and an Intrusion Detection System, which continuously monitor your system. To learn more, please refer to these topics:

- "*Configuring Active Virus Control*" (p. 42)
- "*Configuring the Intrusion Detection System*" (p. 44)

10.1.1. Adjusting the Real-time Protection Level

The real-time protection level defines the scan settings for real-time protection. You can easily change the real-time protection settings according to your needs by switching to one of the predefined protection levels.

To adjust the real-time protection level:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus > Shield**.
3. Drag the slider along the scale to set the desired protection level. Use the description on the right side of the scale to choose the protection level that better fits your security needs.

Note

In Basic View and Intermediate View, you can configure a shortcut so that you can access these settings from your dashboard. For more information, please refer to "*My Tools*" (p. 16).

10.1.2. Creating a Custom Protection Level

Advanced users might want to take advantage of the scan settings Acronis Internet Security offers. The scanner can be set to scan only specific file extensions, to search for specific malware threats or to skip archives. This may greatly reduce scanning times and improve your computer's responsiveness during a scan.

You can configure the real-time protection settings in detail by creating a custom protection level. To create a custom protection level:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus > Shield**.
3. Click **Custom Level**.
4. Configure the scan settings as needed. To find out what an option does, keep the mouse over it and read the description displayed at the bottom of the window.
5. Click **OK** to save the changes and close the window.

You may find this information useful:

- If you are not familiar with some of the terms, check them in the glossary. You can also find useful information by searching the Internet.
- **Scan accessed files.** You can set Acronis Internet Security to scan all accessed files, applications (program files) only or specific file types you consider to be dangerous. Scanning all accessed files provides best protection, while scanning applications only can be used for better system performance.

  Applications (or program files) are far more vulnerable to malware attacks than other types of files. This category includes the following file extensions: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml`; `.nws`.

  If you opt for **Scan user defined extensions**, it is recommended that you include all application extensions beside other file extensions you consider to be dangerous.
- **Scan only new and changed files.** By scanning only new and changed files, you may greatly improve overall system responsiveness with a minimum trade-off in security.
- **Scan boot sectors.** You can set Acronis Internet Security to scan the boot sectors of your hard disk. This sector of the hard disk contains the necessary computer code to start the boot process. When a virus infects the boot sector, the drive may become inaccessible and you may not be able to start your system and access your data.
- **Scan inside archives.** Scanning inside archives is a slow and resource-intensive process, which is therefore not recommended for real-time protection. Archives containing infected files are not an immediate threat to the security of your system. The malware can affect your system only if the infected file is extracted from the archive and executed without having real-time protection enabled.
- **Action options.** If you consider changing the actions taken on detected files, check for tips in *"Changing the Actions Taken on Detected Files"* (p. 41).

- **Scan options for e-mail, web and instant messaging traffic.** To prevent malware from being downloaded to your computer, Acronis Internet Security automatically scans the following malware entry points:
  ▶ incoming e-mails
  ▶ web traffic
  ▶ files received via Yahoo! Messenger and Windows Live Messenger
  Scanning the web traffic may slow down web browsing a little, but it will block malware coming from the Internet, including drive-by downloads.

  Though not recommended, you can disable e-mail, web or instant messaging antivirus scan to increase system performance. If you disable the corresponding scan options, the e-mails and files received or downloaded from the Internet will not be scanned, thus allowing infected files to be saved to your computer. This is not a major threat because real-time protection will block the malware when the infected files are accessed (opened, moved, copied or executed).

10.1.3. Changing the Actions Taken on Detected Files

Files detected by real-time protection are grouped into two categories:

- **Infected files.** Files detected as infected match a malware signature in the Acronis Internet Security Malware Signature Database. Acronis Internet Security can normally remove the malware code from an infected file and reconstruct the original file. This operation is known as disinfection.

  Note
  Malware signatures are snippets of code extracted from actual malware samples. They are used by antivirus programs to perform pattern-matching and detect malware.
  The Acronis Internet Security Malware Signature Database is a collection of malware signatures updated hourly by the Acronis Internet Security malware researchers.

- **Suspicious files.** Files are detected as suspicious by the heuristic analysis. Suspicious files cannot be disinfected, because no disinfection routine is available.

Depending on the type of detected file, the following actions are taken automatically:

- If an infected file is detected, Acronis Internet Security will automatically attempt to disinfect it. If disinfection fails, the file is moved to quarantine in order to contain the infection.

  Important
  For particular types of malware, disinfection is not possible because the detected file is entirely malicious. In such cases, the infected file is deleted from the disk.

- If a suspicious file is detected, access to that file will be denied to prevent a potential infection.

You should not change the default actions taken on detected files unless you have a strong reason to do so.

To change the default actions taken on the infected or suspicious files detected:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus > Shield**.
3. Click **Custom Level**.
4. Configure the actions to be taken on each category of detected files, as needed. The second action is taken if the first one fails (for example, if disinfection is not possible, the infected file is moved to quarantine).

10.1.4. Restoring the Default Settings

The default real-time protection settings ensure good protection against malware, with minor impact on system performance.

To restore the default real-time protection settings:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus > Shield**.
3. Click **Default Level**.

10.1.5. Configuring Active Virus Control

The Acronis Internet Security Active Virus Control detects potentially harmful applications based on their behavior.

Active Virus Control continuously monitors the applications running on the computer, looking for malware-like actions. Each of these actions is scored and an overall score is computed for each process. When the overall score for a process reaches a given threshold, the process is considered to be harmful. Depending on the program settings, the process is blocked automatically or you may prompted to specify the action to be taken.

Active Virus Control can be configured to alert you and prompt you for action whenever an application tries to perform a possible malicious action.

If you know and trust the detected application, click **Allow**.

If you want to immediately close the application, click **OK**.

Select the **Remember this action for this application** check box before making your choice and Acronis Internet Security will take the same action for the detected application in the future. The rule that is thus created will be listed in the Active Virus Control configuration window.

To configure Active Virus Control:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus > Shield**.
3. Click **Advanced Settings**.
4. Go to the **AVC** tab.
5. Select the corresponding check box to enable Active Virus Control.
6. Drag the slider along the scale to set the desired protection level. Use the description on the right side of the scale to choose the protection level that better fits your security needs.

Adjusting the Aggressiveness Level

To configure the Active Virus Control protection level:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus > Shield**.
3. Click **Advanced Settings**.
4. Go to the **AVC** tab.
5. Drag the slider along the scale to set the desired protection level. Use the description on the right side of the scale to choose the protection level that better fits your security needs.

Configuring the Response to Malicious Behavior

If an application exhibits malicious behavior, you will be prompted whether to allow or block it.

To configure the response to malicious behavior:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus > Shield**.
3. Click **Advanced Settings**.
4. Go to the **AVC** tab.
5. If you want to be prompted for action when Active Virus Control detects a potentially harmful application, select the **Alert me before taking an action** check box. To automatically block an application that exhibits malicious behavior (without displaying an alert window), clear this check box.

Managing Trusted / Untrusted Applications

You can add applications you know and trust to the list of trusted applications. These applications will no longer be checked by the Acronis Internet Security Active Virus Control and will automatically be allowed access.

To manage the applications that are not being monitored by Active Virus Control:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus > Shield**.
3. Click **Advanced Settings**.
4. Go to the **AVC** tab.
5. Click the **Exclusions** tab.

The applications for which rules have been created are listed in the **Exclusions** table. The path to the application and the action you have set for it (Allowed or Blocked) is displayed for each rule.

To change the action for an application, click the current action and select the other action from the menu.

To manage the list, use the buttons placed above the table:

- **Add** - add a new application to the list.
- **Remove** - remove an application from the list.
- **Edit** - edit an application rule.

10.1.6. Configuring the Intrusion Detection System

The Acronis Internet Security Intrusion Detection System monitors network and system activities for malicious activities or policy violations.

To configure the Intrusion Detection System:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus > Shield**.
3. Click **Advanced Settings**.
4. Go to the **IDS** tab.
5. Select the corresponding check box to enable the Intrusion Detection System.
6. Drag the slider along the scale to set the desired aggressiveness level. Use the description on the right side of the scale to choose the aggressiveness level that better fits your security needs.

10.2. On-demand Scanning

The main objective for Acronis Internet Security is to keep your computer clean of viruses. This is first and foremost done by keeping new viruses out of your computer and by scanning your e-mail messages and any new files downloaded or copied to your system.

There is a risk that a virus is already lodged in your system, before you even install Acronis Internet Security. This is why it's a very good idea to scan your computer for resident viruses after you've installed Acronis Internet Security. And it's definitely a good idea to frequently scan your computer for viruses.

On-demand scanning is based on scan tasks. Scan tasks specify the scanning options and the objects to be scanned. You can scan the computer whenever you want by running the default tasks or your own scan tasks (user-defined tasks). You can also schedule them to run on a regular basis or when the system is idle so as not to interfere with your work. For quick instructions, please refer to these topics:

- "*How Do I Scan Files and Folders?*" (p. 140)
- "*How Do I Create a Custom Scan Task?*" (p. 142)
- "*How Do I Schedule a Computer Scan?*" (p. 143)

10.2.1. Scanning Files and Folders

You should scan files and folders whenever you suspect they might be infected. Right-click the file or folder you want to be scanned and select **Scan with Acronis Internet Security**. The Antivirus Scan wizard will appear and guide you through the scanning process.

If you want to scan specific locations on your computer, you can configure and run a custom scan task. For more information, please refer to "*How Do I Create a Custom Scan Task?*" (p. 142).

To scan your computer or part of it you can run the default scan tasks or your own scan tasks. To run a scan task, open Acronis Internet Security and, depending on the user interface view mode, proceed as follows:

Basic View
: Click the **Security** button and choose one of the available scan tasks.

Intermediate View
: Go to the **Security** tab. Click **Full System Scan** in the left-side Quick Tasks area and choose one of the available scan tasks.

Expert View
: Go to **Antivirus > Virus Scan**. To run a system or user-defined scan task, click the corresponding **Run Task** button.

These are the default tasks you can use to scan your computer:

Full System Scan
Scans the entire system, except for archives. In the default configuration, it scans for all types of malware other than rootkits.

Quick Scan
Quick Scan uses in-the-cloud scanning to detect malware running in your system. Running a Quick Scan usually takes less than a minute and uses a fraction of the system resources needed by a regular virus scan.

Deep System Scan
Scans the entire system. In the default configuration, it scans for all types of malware threatening your system's security, such as viruses, spyware, adware, rootkits and others.

Before you initiate a scanning process, you should make sure that Acronis Internet Security is up to date with its malware signatures. Scanning your computer using an outdated signature database may prevent Acronis Internet Security from detecting new malware found since the last update.

In order for Acronis Internet Security to make a complete scanning, you need to shut down all open programs. Especially your email-client (i.e. Outlook, Outlook Express or Eudora) is important to shut down.

Scanning Tips

Here are some more scanning tips you may find useful:

- Depending on the size of your hard disk, running a comprehensive scan of your computer (such as Deep System Scan or System Scan) may take a while (up to an hour or even more). Therefore, you should run such scans when you do not need to use your computer for a longer time (for example, during the night).

  You can schedule the scan to start when convenient. Make sure you leave your computer running. With Windows Vista, make sure your computer is not in sleep mode when the task is scheduled to run.

- If you frequently download files from the Internet to a specific folder, create a new scan task and set that folder as scan target. Schedule the task to run every day or more often.

- There is a kind of malware which sets itself to be executed at system startup by changing Windows settings. To protect your computer against such malware, you can schedule the **Auto-logon Scan** task to run at system startup. Please note that autologon scanning may affect system performance for a short time after startup.

10.2.2. Antivirus Scan Wizard

Whenever you initiate an on-demand scan (for example, right-click a folder and select **Scan with Acronis Internet Security**), the Acronis Internet Security

Antivirus Scan wizard will appear. Follow the three-step guided procedure to complete the scanning process.

Note

If the scan wizard does not appear, the scan may be configured to run silently, in the background. Look for the scan progress icon in the system tray. You can click this icon to open the scan window and to see the scan progress.

Step 1/3 - Scanning

Acronis Internet Security will start scanning the selected objects.

You can see the scan status and statistics (scanning speed, elapsed time, number of scanned / infected / suspicious / hidden objects and other).

Wait for Acronis Internet Security to finish scanning.

Note

The scanning process may take a while, depending on the complexity of the scan.

Password-protected archives. When a password-protected archive is detected, depending on the scan settings, you may be prompted to provide the password. Password-protected archives cannot be scanned unless you provide the password. The following options are available:

- **I want to enter the password for this object.** If you want Acronis Internet Security to scan the archive, select this option and type the password. If you do not know the password, choose one of the other options.
- **I do not want to enter the password for this object (skip this object).** Select this option to skip scanning this archive.
- **I do not want to enter the password for any object (skip all password-protected objects).** Select this option if you do not want to be bothered about password-protected archives. Acronis Internet Security will not be able to scan them, but a record will be kept in the scan log.

Click **OK** to continue scanning.

Stopping or pausing the scan. You can stop scanning anytime you want by clicking **Stop&Yes**. You will go directly to the last step of the wizard. To temporarily stop the scanning process, just click **Pause**. You will have to click **Resume** to resume scanning.

Step 2/3 - Select Actions

When the scanning is completed, a new window will appear, where you can see the scan results.

If there are no unresolved threats, click **Continue**. Otherwise, you must configure new actions to be taken on the unresolved threats in order to protect your system.

The infected objects are displayed in groups, based on the malware they are infected with. Click the link corresponding to a threat to find out more information about the infected objects.

You can choose an overall action to be taken for all issues or you can select separate actions for each group of issues. One or several of the following options can appear on the menu:

Take No Action
No action will be taken on the detected files. After the scan is completed, you can open the scan log to view information on these files.

Disinfect
Removes the malware code from infected files.

Delete
Removes detected files from the disk.

Move to quarantine
Moves detected files to quarantine. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. For more information, please refer to "*Quarantine Area*" (p. 58).

Rename files
Changes the name of hidden files by appending `.bd.ren` to their name. As a result, you will be able to search for and find such files on your computer, if any.

Please note that these hidden files are not the files that you deliberately hide from Windows. They are the files hidden by special programs, known as rootkits. Rootkits are not malicious in nature. However, they are commonly used to make viruses or spyware undetectable by normal antivirus programs.

Click **Continue** to apply the specified actions.

Step 3/3 - View Results

When Acronis Internet Security finishes fixing the issues, the scan results will appear in a new window. If you want comprehensive information on the scanning process, click **Show Log** to view the scan log.

Important
If required, please restart your system in order to complete the cleaning process.

Click **Close** to close the window.

Acronis Internet Security Could Not Solve Some Issues

In most cases Acronis Internet Security successfully disinfects the infected files it detects or it isolates the infection. However, there are issues that cannot be solved automatically. For more information and instructions on how to remove malware manually, please refer to "*Removing Malware from Your System*" (p. 164).

Acronis Internet Security Detected Suspect Files

Suspect files are files detected by the heuristic analysis as potentially infected with malware the signature of which has not been released yet.

If suspect files were detected during the scan, you will be requested to submit them to the Acronis Internet Security Lab. Click **OK** to send these files to the Acronis Internet Security Lab for further analysis.

10.2.3. Viewing Scan Logs

Each time you perform a scan, a scan log is created. The scan log contains detailed information about the logged scanning process, such as scanning options, the scanning target, the threats found and the actions taken on these threats.

You can open the scan log directly from the scan wizard, once the scan is completed, by clicking **Show Log**.

To check scan logs at a later time:

1. Open Acronis Internet Security.
2. Click the **View Logs** link in the bottom-right corner of the window.
3. Click **Antivirus** on the left-side menu.
4. In the **On-demand Tasks** section, you can check what scans have been performed recently. Double-click the events in the list to see more details. To open the scan log, click **View Scan Log**. The scan log will open in your default web browser.

To delete a log entry, right-click it and select **Delete**.

10.2.4. Managing Existing Scan Tasks

Acronis Internet Security comes with several tasks, created by default, which cover common security issues. You can also create your own customized scan tasks. For more information, please refer to "*How Do I Create a Custom Scan Task?*" (p. 142).

To manage the existing scan tasks:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus > Virus Scan**.

Note

In Basic View and Intermediate View, you can configure a shortcut so that you can access these settings from your dashboard. For more information, please refer to "*My Tools*" (p. 16).

There are three categories of scan tasks:

- **System tasks** - contains the list of default system tasks. The following tasks are available:

  Full System Scan
  Scans the entire system, except for archives. In the default configuration, it scans for all types of malware other than rootkits.

  Quick Scan
  Quick Scan uses in-the-cloud scanning to detect malware running in your system. Running a Quick Scan usually takes less than a minute and uses a fraction of the system resources needed by a regular virus scan.

  Auto-logon Scan
  Scans the items that are run when a user logs on to Windows. By default, the autologon scan is disabled.

  If you want to use this task, right-click it, select **Schedule** and set the task to run **at system startup**. You can specify how long after the startup the task should start running (in minutes).

  Deep System Scan
  Scans the entire system. In the default configuration, it scans for all types of malware threatening your system's security, such as viruses, spyware, adware, rootkits and others.

  Note

  Since the **Deep System Scan** and **Full System Scan** tasks analyze the entire system, the scanning may take a while. Therefore, we recommend you to run these tasks on low priority or, better, when your system is idle.

- **User tasks** - contains the user-defined tasks.

  A task called `My Documents` is provided. Use this task to scan important current user folders: `My Documents`, `Desktop` and `StartUp`. This will ensure the safety of your documents, a safe workspace and clean applications running at startup.

- **Misc tasks** - contains a list of miscellaneous scan tasks. These scan tasks refer to alternative scanning types that cannot be run from this window. You can only modify their settings or view the scan reports. The following tasks are available:

Device Scanning

Acronis Internet Security can detect automatically when a new storage device is connected to the computer and scan it. Use this task to configure the options of the automatic detection and scanning of storage devices (CDs/DVDs, USB storage devices or mapped network drives).

Contextual Scan

This task is used when scanning via the Windows contextual menu or using the scan activity bar. You can modify the scan options to better suit your needs.

- **Idle Scan Tasks** - contains a list of default system tasks which can be scheduled to run when you are away from your computer. With complex tasks, the scanning process will take some time and it will work best if you don't use your system during that time. That is why you should schedule such tasks when your computer has gone into the idle mode.

You can manage scan tasks using the buttons or the shortcut menu.

To run a system or user-defined scan task, click the corresponding **Run Task** button. The Antivirus Scan wizard will appear and guide you through the scanning process.

To set a scan task to run automatically, at a later moment or regularly, click the corresponding **Schedule** button and configure the task schedule as needed.

If you no longer need a scan task that you have created (a user-defined task), you can delete it by clicking the **Delete** button, located to the right of the task. You cannot remove system or miscellaneous tasks.

Each scan task has a Properties window where you can configure its settings and view the scan logs. To open this window click the **Properties** button to the left of the task (or right-click the task and then click **Properties**).

To learn more, please refer to these topics:

- "*Configuring Scan Settings*" (p. 52)
- "*Setting Scan Target*" (p. 54)
- "*Scheduling Scan Tasks*" (p. 55)

Using Shortcut Menu

A shortcut menu is available for each task. Right-click the selected task to open it.

For system and user-defined tasks, the following commands are available on the shortcut menu:

- **Scan Now** - runs the selected task, initiating an immediate scan.
- **Paths** - opens the **Properties** window, Paths tab, where you can change the scan target of the selected task. In the case of system tasks, this option is replaced by **Show Scan Paths**, as you can only see their scan target.

- **Schedule** - opens the **Properties** window, Scheduler tab, where you can schedule the selected task.
- **View Logs** - opens the **Properties** window, Logs tab, where you can see the reports generated after the selected task was run.
- **Clone Task** - duplicates the selected task. This is useful when creating new tasks, as you can modify the settings of the task duplicate.
- **Delete** - deletes the selected task.

Note
Available for user-created tasks only. You cannot remove a default task.

- **Properties** - opens the **Properties** window, Overview tab, where you can change the settings of the selected task.

Due to the particular nature of the **Misc Tasks** category, only the **View Logs** and **Properties** options are available in this case.

Configuring Scan Settings

To configure the scanning options of a specific scan task, right-click it and select **Properties**.

You can easily configure the scanning options by adjusting the scan level. Drag the slider along the scale to set the desired scan level. Use the description on the right side of the scale to identify the scan level that better fits your needs.

You can also configure these general options:

- **Run the task with Low priority.** Decreases the priority of the scan process. You will allow other programs to run faster and increase the time needed for the scan process to finish.
- **Minimize Scan Wizard to system tray.** Minimizes the scan window to the system tray. Double-click the Acronis Internet Security icon to open it.
- Specify the action to be taken if no threats are found.

Advanced users might want to take advantage of the scan settings Acronis Internet Security offers. The scanner can be set to scan only specific file extensions, to search for specific malware threats or to skip archives. This may greatly reduce scanning times and improve your computer's responsiveness during a scan.

To configure the scan settings in detail:

1. Click **Custom**.
2. Configure the scan settings as needed. To find out what an option does, keep the mouse over it and read the description displayed at the bottom of the window.

3. Click **OK** to save the changes and close the window.

You may find this information useful:

- If you are not familiar with some of the terms, check them in the glossary. You can also find useful information by searching the Internet.
- **Scan Level.** Specify the type of malware you want Acronis Internet Security to scan for by selecting the appropriate options.
- **Scan files.** You can set Acronis Internet Security to scan all types of files, applications (program files) only or specific file types you consider to be dangerous. Scanning all files provides best protection, while scanning applications only can be used to perform a quicker scan.

  Applications (or program files) are far more vulnerable to malware attacks than other types of files. This category includes the following file extensions: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml`; `.nws`.

  If you opt for **Scan user defined extensions**, it is recommended that you include all application extensions beside other file extensions you consider to be dangerous.
- **Scan only new and changed files.** By scanning only new and changed files, you may greatly improve overall system responsiveness with a minimum trade-off in security.
- **Scan inside archives.** Archives containing infected files are not an immediate threat to the security of your system. The malware can affect your system only if the infected file is extracted from the archive and executed without having real-time protection enabled. However, it is recommended to use this option in order to detect and remove any potential threat, even if it is not an immediate threat.

  Note

  Scanning archived files increases the overall scanning time and requires more system resources.

- **Action options.** Specify the actions to be taken on each category of detected files using the options in this category. There are three categories of detected files:

  ▶ **Infected files.** Files detected as infected match a malware signature in the Acronis Internet Security Malware Signature Database. Acronis Internet Security

can normally remove the malware code from an infected file and reconstruct the original file. This operation is known as disinfection.

Note

Malware signatures are snippets of code extracted from actual malware samples. They are used by antivirus programs to perform pattern-matching and detect malware.

The Acronis Internet Security Malware Signature Database is a collection of malware signatures updated hourly by the Acronis Internet Security malware researchers.

- **Suspicious files.** Files are detected as suspicious by the heuristic analysis. Suspicious files cannot be disinfected, because no disinfection routine is available.
- **Hidden files (rootkits).** Please note that these hidden files are not the files that you deliberately hide from Windows. They are the files hidden by special programs, known as rootkits. Rootkits are not malicious in nature. However, they are commonly used to make viruses or spyware undetectable by normal antivirus programs.

You should not change the default actions taken on detected files unless you have a strong reason to do so.

To set a new action, click the current **First action** and select the desired option from the menu. Specify a **Second action** that will be taken in case the first one fails.

Click **OK** to save the changes and close the window. To run the task, just click **Scan**.

Setting Scan Target

You cannot modify the scan target of the scan tasks from the **System Tasks** category. You can only see their scan target. To view the scan target of a specific system scan task, right-click the task and select **Show Scan Paths**.

To set the scan target of a specific user scan task, right-click the task and select **Paths**. Alternatively, if you are already in the Properties window of a task, select the **Paths** tab.

You can see the list of local, network and removable drives as well as the files or folders added previously, if any. All checked items will be scanned when running the task.

The following buttons are available:

- **Add Item(s)** - opens a browsing window where you can select the file(s) / folder(s) that you want to be scanned.

Note

You can also use drag and drop to add files/folders to the list.

- **Delete Item(s)** - removes the file(s) / folder(s) previously selected from the list of objects to be scanned.

Besides these buttons, there are some options that allow the fast selection of the scan locations.

- **Local Drives** - to scan the local drives.
- **Network Drives** - to scan all network drives.
- **Removable Drives** - to scan removable drives (CD-ROM, floppy-disk unit).
- **All Entries** - to scan all drives, no matter if they are local, in the network or removable.

Click **OK** to save the changes and close the window. To run the task, just click **Scan**.

Scheduling Scan Tasks

To see the schedule of a specific task or to modify it, choose a task and select **Schedule**. If you are already in a task's Properties window, select the **Scheduler** tab.

You can see the task schedule, if any.

When scheduling a task, you must choose one of the following options:

- **No** - launches the task only when the user requests it.
- **Once** - launches the scan only once, at a certain moment. Specify the start date and time in the **Start Date/Time** fields.
- **Periodically** - launches the scan periodically, at certain time intervals(minutes, hours, days, weeks, months) starting with a specified date and time.
- **At system startup** - launches the scan at the specified number of minutes after a user has logged on to Windows.

Click **OK** to save the changes and close the window. To run the task, just click **Scan**.

10.3. Configuring Scan Exclusions

There are cases when you may need to exclude certain files from scanning. For example, you may want to exclude an EICAR test file from on-access scanning or `.avi` files from on-demand scanning.

Acronis Internet Security allows excluding objects from on-access or on-demand scanning, or from both. This feature is intended to decrease scanning times and to avoid interference with your work.

Two types of objects can be excluded from scanning:

- **Paths** - the file or the folder (including all the objects it contains) indicated by a specified path will be excluded from scanning.
- **Extensions** - all files having a specific extension will be excluded from scanning, no matter what their location on the hard drive.

The objects excluded from on-access scanning will not be scanned, no matter if they are accessed by you or by an application.

Note

Exclusions will NOT apply for contextual scanning. Contextual scanning is a type of on-demand scanning: you right-click the file or folder you want to scan and select **Scan with Acronis Internet Security**.

10.3.1. Excluding Files or Folders from Scanning

To exclude paths from scanning:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus > Exclusions**.

Note

In Basic View and Intermediate View, you can configure a shortcut so that you can access these settings from your dashboard. For more information, please refer to "*My Tools*" (p. 16).

3. Select the corresponding check box to enable scan exclusions.
4. Start the configuration wizard as follows:
   - Right-click in the Files and Folders table and select **Add new path**.
   - Click the **Add** button, located at the top of the exclusions table.
5. Follow the configuration wizard. You can navigate through the wizard using the **Next** and **Back** buttons. To exit the wizard, click **Cancel**.
   a. Select the option of excluding a path from scanning. This step appears only when you start the wizard by clicking the **Add** button.
   b. To specify the paths to be excluded from scanning use either of the following methods:
      - Click **Browse**, select the file or folder that you want to be excluded from scanning and then click **Add**.
      - Type the path that you want to be excluded from scanning in the edit field and click **Add**.

      The paths will appear in the table as you add them. You can add as many paths as you want.

c. By default, the selected paths are excluded from both on-access and on-demand scanning. To change when to apply the exception, click on the right column and select the desired option from the list.

d. It is highly recommended to scan the files in the specified paths to make sure that they are not infected. Select the check box to scan these files before excluding them from scanning.

Click **Finish** to add the scan exclusions.

6. Click **Apply** to save the changes.

10.3.2. Excluding File Extensions from Scanning

To exclude file extensions from scanning:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus > Exclusions**.

Note

In Basic View and Intermediate View, you can configure a shortcut so that you can access these settings from your dashboard. For more information, please refer to "*My Tools*" (p. 16).

3. Select the corresponding check box to enable scan exclusions.
4. Start the configuration wizard as follows:
   - Right-click in the Extensions table and select **Add new extensions**.
   - Click the **Add** button, located at the top of the exclusions table.
5. Follow the configuration wizard. You can navigate through the wizard using the **Next** and **Back** buttons. To exit the wizard, click **Cancel**.
   a. Select the option of excluding extensions from scanning. This step appears only when you start the wizard by clicking the **Add** button.
   b. To specify the extensions to be excluded from scanning use either of the following methods:
      - Select from the menu the extension that you want to be excluded from scanning and then click **Add**.

Note

The menu contains a list of all the extensions registered on your system. When you select an extension, you can see its description, if available.

      - Type the extension that you want to be excluded from scanning in the edit field and click **Add**.

The extensions will appear in the table as you add them. You can add as many extensions as you want.

c. By default, the selected extensions are excluded from both on-access and on-demand scanning. To change when to apply the exception, click on the right column and select the desired option from the list.

d. It is highly recommended to scan the files with the specified extensions to make sure that they are not infected.

Click **Finish** to add the scan exclusions.

6. Click **Apply** to save the changes.

10.3.3. Managing Scan Exclusions

If the configured scan exclusions are no longer needed, it is recommended that you delete them or disable scan exclusions.

To manage scan exclusions:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus > Exclusions**.

To remove an entry from the table, select it and click the **Delete** button.

To edit an entry from the table, select it and click the **Edit** button. A new window will appear where you can change the extension or the path to be excluded and the type of scanning you want them to be excluded from, as needed. Make the necessary changes and click **OK**.

Note
You can also right-click an object and use the options on the shortcut menu to edit or delete it.

To disable scan exclusions, clear the corresponding check box.

10.4. Quarantine Area

Acronis Internet Security allows isolating the infected or suspicious files in a secure area, named quarantine. By isolating these files in the quarantine, the risk of getting infected disappears and, at the same time, you have the possibility to send these files for further analysis to the Acronis Internet Security lab.

Note
When a virus is in quarantine it cannot do any harm because it cannot be executed or read.

In addition, Acronis Internet Security scans the quarantined files after each malware signature update. Cleaned files are automatically moved back to their original location.

To see and manage quarantined files and to configure the quarantine settings:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus > Quarantine**.

Note

In Basic View and Intermediate View, you can configure a shortcut so that you can access these settings from your dashboard. For more information, please refer to "*My Tools*" (p. 16).

Managing Quarantined Files

You can send any selected file from the quarantine to the Acronis Internet Security Lab by clicking **Send**. By default, Acronis Internet Security will automatically submit quarantined files every 60 minutes.

To delete a quarantined file, select it and click the **Delete** button.

If you want to restore a quarantined file to its original location, select it and click **Restore**.

Configuring Quarantine Settings

To configure the quarantine settings, click **Settings**. Using the quarantine settings, you can set Acronis Internet Security to automatically perform the following actions:

Delete old files. To automatically delete old quarantined files, check the corresponding option. You must specify the number of days after which the quarantined files should be deleted and frequency with which Acronis Internet Security should check for old files.

Automatically submit files. To automatically submit quarantined files, check the corresponding option. You must specify the frequency with which to submit files.

Scan quarantined files after update. To automatically scan quarantined files after each update performed, check the corresponding option. You can choose to automatically move back the cleaned files to their original location by selecting **Restore clean files**.

Click **OK** to save the changes and close the window.

11. Antiphishing Protection

Acronis Internet Security Antiphishing prevents you from disclosing personal information while browsing the Internet by alerting you about potential phishing web pages.

Acronis Internet Security provides real-time antiphishing protection for:

- Internet Explorer
- Mozilla Firefox
- Yahoo! Messenger
- Windows Live (MSN) Messenger

11.1. Configuring the Antiphishing White List

You can configure and manage a white list of web sites that will not be scanned by the Acronis Internet Security Antiphishing engines. The white list should contain only web sites you fully trust. For example, add the web sites where you currently shop online.

Note

You can easily add web sites to the white list from the Acronis Internet Security Antiphishing toolbar integrated into your web browser. For more information, please refer to "*Managing the Acronis Internet Security Antiphishing Protection in Internet Explorer and Firefox*" (p. 61).

To configure and manage the antiphishing white list:

- If you are using a supported web browser, click the Acronis Internet Security toolbar and choose **White List** from the menu.
- Alternatively, follow these steps:
  1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
  2. Go to **Antivirus > Shield**.
  3. Click **White List**.

To add a site to the White List, provide its address in the corresponding field and click **Add**.

If you want to remove a web site from the white list, click the corresponding **Remove** button.

Click **Save** to save the changes and close the window.

11.2. Managing the Acronis Internet Security Antiphishing Protection in Internet Explorer and Firefox

Acronis Internet Security integrates directly through an intuitive and easy-to-use toolbar into the following web browsers:

- Internet Explorer
- Mozilla Firefox

You can easily and efficiently manage antiphishing protection and the White List using the Acronis Internet Security Antiphishing toolbar integrated into one of the above web browsers.

The antiphishing toolbar, represented by the Acronis Internet Security icon, is located on the topside of browser. Click it in order to open the toolbar menu.

Note
If you cannot see the toolbar, open the **View** menu, point to **Toolbars** and check **Acronis Internet Security Toolbar**.

The following commands are available on the toolbar menu:

- **Enable / Disable** - enables / disables the Acronis Internet Security antiphishing protection in the current web browser.
- **Settings** - opens a window where you can specify the antiphishing toolbar's settings. The following options are available:
  - ▶ **Real-time Antiphishing Web Protection** - detects and alerts you in real-time if a web site is phished (set up to steal personal information). This option controls the Acronis Internet Security antiphishing protection in the current web browser only.
  - ▶ **Ask before adding to whitelist** - prompts you before adding a web site to the White List.
- **Add to White List** - adds the current web site to the White List.

Important
Adding a site to the White List means that Acronis Internet Security will not scan the site for phishing attempts anymore. We recommend you to add to the White List only sites that you fully trust.

- **White List** - opens the White List. For more information, please refer to *"Configuring the Antiphishing White List" (p. 60)*.
- **Report as Phishing** - informs the Acronis Internet Security Lab that you consider the respective web site to be used for phishing. By reporting phished web sites you help protect other people against identity theft.
- **Help** - opens the help file.

- **About** - opens a window where you can see information about Acronis Internet Security and where to look for help in case something unexpected appears.

12. Search Advisor

Search Advisor improves your online threat protection by alerting you about phishing or untrusted web pages directly from your search results page.

Search Advisor works with any web browser and checks the search results displayed by the most popular search engines:

- Google
- Yahoo!
- Bing

Search Advisor indicates whether a search result is safe or not by placing a small status icon before the link.

Green circle with a check mark: You can safely access the link.

Red circle with an exclamation mark: This is a phishing or untrusted web page. You should avoid opening the link. If you are using Internet Explorer or Firefox and you try to open the link, Acronis Internet Security will automatically block the web page and display an alert page instead. If you want to ignore the alert and access the web page, follow the instructions in the alert page.

12.1. Disabling Search Advisor

To disable Search Advisor:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Preferences**.
2. Go to **Security Settings**.
3. Use the switch to turn off Search Advisor.

13. Antispam

Spam is a term used to describe unsolicited e-mail. Spam is a growing problem, both for individuals and for organizations. It's not pretty, you wouldn't want your kids to see it, it can get you fired (for wasting too much time or from receiving porn in your office mail) and you can't stop people from sending it. The next best thing to that is, obviously, to stop receiving it. Unfortunately, Spam comes in a wide range of shapes and sizes, and there's a lot of it.

Acronis Internet Security Antispam employs remarkable technological innovations and industry standard antispam filters to weed out spam before it reaches the user's Inbox. For more information, please refer to "*Antispam Insights*" (p. 64).

The Acronis Internet Security Antispam protection is available only for e-mail clients configured to receive e-mail messages via the POP3 protocol. POP3 is one of the most widely used protocols for downloading e-mail messages from a mail server.

Note
Acronis Internet Security does not provide antispam protection for e-mail accounts that you access through a web-based e-mail service.

The spam messages detected by Acronis Internet Security are marked with the `[spam]` prefix in the subject line. Acronis Internet Security automatically moves spam messages to a specific folder, as follows:

- In Microsoft Outlook, spam messages are moved to a **Spam** folder, located in the **Deleted Items** folder. The **Spam** folder is created during the installation of Acronis Internet Security.
- In Outlook Express and Windows Mail, spam messages are moved directly to **Deleted Items**.
- In Mozilla Thunderbird, spam messages are moved to a **Spam** folder, located in the **Trash** folder. The **Spam** folder is created during the installation of Acronis Internet Security.

If you use other mail clients, you must create a rule to move the e-mail messages marked as `[spam]` by Acronis Internet Security to a custom quarantine folder.

13.1. Antispam Insights

13.1.1. Antispam Filters

The Acronis Internet Security Antispam Engine incorporates several different filters that ensure your Inbox to be SPAM-free: Friends list, Spammers list, Charset filter, Image filter, URL filter, NeuNet (Heuristic) filter and Bayesian filter.

Friends List / Spammers List

Most people communicate regularly to a group of people or even receive messages from companies or organizations in the same domain. By using **friends or spammers list**, you can easily classify which people you want to receive e-mail from (friends) no matter what the message contains, or which people you never want to hear from again (spammers).

Note

We recommend that you add your friends' names and e-mail addresses to the **Friends list**. Acronis Internet Security does not block messages from those on the list; therefore, adding friends helps ensure that legitimate messages get through.

Charset Filter

Many spam messages are written in Cyrillic and / or Asian charsets. The Charset Filter detects this kind of messages and tags them as SPAM.

Image Filter

Since avoiding heuristic filter detection has become quite a challenge, nowadays' inbox folders are full with more and more messages only containing an image with unsolicited content. To cope with this growing problem, Acronis Internet Security introduced the **Image filter** that compares the image signature from the e-mail with those from the Acronis Internet Security database. In case of a match the e-mail will be tagged as SPAM.

URL Filter

Almost all spam messages include links to various web locations. These locations usually contain more advertising and the possibility to buy things, and, sometimes, they are used for phishing.

Acronis Internet Security maintains a database of such links. The URL filter checks every URL link in a message against its database. If a match is made, the message is tagged as SPAM.

NeuNet (Heuristic) Filter

The **NeuNet (Heuristic) filter** performs a set of tests on all the message components, (i.e. not only the header but also the message body in either HTML or text format), looking for words, phrases, links or other characteristics of SPAM. Based on the results of the analysis, it adds a SPAM score to the message.

The filter also detects messages marked as `SEXUALLY-EXPLICIT:` in the subject line and tags them as SPAM.

Note

Starting May 19, 2004, spam that contains sexually oriented material must include the warning SEXUALLY-EXPLICIT: in the subject line or face fines for violations of federal law.

Bayesian Filter

The **Bayesian filter** module classifies messages according to statistical information regarding the rate at which specific words appear in messages classified SPAM as compared to those declared NON-SPAM (by you or by the heuristic filter).

This means, for example, if a certain four-letter word is seen to appear more often in SPAM, it is natural to assume there is an increased probability that the next incoming message that includes it actually IS SPAM. All relevant words within a message are taken into account. By synthesizing the statistical information, the overall probability for the whole message to be SPAM is computed.

This module presents another interesting characteristic: it is trainable. It adapts quickly to the type of messages received by a certain user, and stores information about all. To function effectively, the filter must be trained, meaning, to be presented with samples of SPAM and legitimate messages, much like a hound is primed to trace a certain scent. Sometimes the filter must be corrected too - prompted to adjust when it makes a wrong decision.

Important

You can correct the Bayesian filter using the **Is Spam** and **Not Spam** buttons from the Antispam toolbar.

13.1.2. Antispam Operation

The Acronis Internet Security Antispam Engine uses all antispam filters combined to determine whether a certain e-mail message should get into your **Inbox** or not.

Every e-mail that comes from the Internet is first checked with the Friends list/Spammers list filter. If the sender's address is found in the Friends list the e-mail is moved directly to your **Inbox**.

Otherwise, the Spammers list filter will take over the e-mail to verify if the sender's address is on its list. If a match is made, the e-mail will be tagged as SPAM and moved in the **Spam** folder.

Else, the Charset filter will check if the e-mail is written in Cyrillic or Asian characters. If so the e-mail will be tagged as SPAM and moved in the **Spam** folder.

If the e-mail is not written in Asian or Cyrillic it will be passed to the Image filter. The **Image filter** will detect all the e-mail messages containing attached images with spam content.

The URL filter will compare the links found in the e-mail against the links from the Acronis Internet Security database of known spam links. In case of a match, the e-mail will be considered SPAM.

The NeuNet (Heuristic) filter will take over the e-mail and will perform a set of tests on all the message components, looking for words, phrases, links or other characteristics of SPAM. Based on the results of the analysis, the e-mail will receive a spam score.

Note

If the e-mail is tagged as SEXUALLY EXPLICIT in the subject line, Acronis Internet Security will consider it SPAM.

The Bayesian filter module will further analyze the message, according to statistical information regarding the rate at which specific words appear in messages classified SPAM as compared to those declared NON-SPAM (by you or by the heuristic filter). A Spam score will be added to the e-mail.

If the aggregate spam score (heuristic score + Bayesian score) exceeds the threshold level, the e-mail is considered SPAM. The threshhold level is defined by the antispam protection level. For more information, please refer to *"Adjusting the Protection Level" (p. 72)*.

13.1.3. Antispam Updates

Every time you perform an update:

- new image signatures will be added to the **Image filter**.
- new links will be added to the **URL filter**.
- new rules will be added to the **NeuNet (Heuristic) filter**.

This will help increase the effectiveness of your Antispam engine.

To protect you against spammers, Acronis Internet Security can perform automatic updates. Keep the **Automatic Update** option enabled.

13.1.4. Supported E-mail Clients and Protocols

Antispam protection is provided for all POP3/SMTP e-mail clients. The Acronis Internet Security Antispam toolbar however is integrated only into:

- Microsoft Outlook 2003 / 2007 / 2010
- Microsoft Outlook Express
- Microsoft Windows Mail
- Mozilla Thunderbird 3.0.4

Note

Acronis Internet Security 2011 doesn't scan Lotus Notes POP3 traffic.

13.2. Antispam Optimization Wizard

The first time you run your mail client after you have installed Acronis Internet Security, a wizard will appear helping you to configure the Friends list and the Spammers list and to train the Bayesian filter in order to increase the efficiency of the Antispam filters.

Note
The wizard can also be launched any time you want by clicking the **Wizard** button from the Antispam toolbar.

You can navigate through the wizard using the **Next** and **Back** buttons. If you want to skip a configuration step, select **Skip this step**. To exit the wizard, click **Cancel**.

1. **Welcome Window**
2. **Add Contacts to Friends List**

   Here you can see all the addresses from your **Address Book**. Please select those you want to be added to your **Friends list** (we recommend to select them all). You will receive all the e-mail messages from these addresses, regardless of their content.

   To add all your contacts to the Friends list, check **Select all**.
3. **Delete Bayesian Database**

   Note
   The first time you run the wizard, just go to the next step.

   You may find that your antispam filter has begun to lose efficiency. This may be due to improper training. (i.e. you have mistakenly tagged a number of legitimate messages as spam, or vice versa). If your filter is very inaccurate, you may need to wipe the filter database and retrain the filter by following the next steps of this wizard.

   Select **Wipe antispam filter database** if you want to reset the Bayesian database.

   You can save the Bayesian database to a file so that you can use it with another Acronis Internet Security product or after reinstalling Acronis Internet Security. To save the Bayesian database, click the **Save Bayes** button and save it to the desired location. The file will have a `.dat` extension.

   To load a previously saved Bayesian database, click the **Load Bayes** button and open the corresponding file.
4. **Train the Bayesian Filter on Legitimate (Non-Spam) E-mails**

Please select a folder that contains legitimate e-mail messages. These messages will be used to train the antispam filter.

There are two advanced options under the directory list:
- **Include all subfolders** - to include the subfolders to your selection.
- **Automatically add to Friends list** - to add the senders to the Friends list.

5. **Train the Bayesian Filter on Spam E-mails**

   Please select a folder that contains spam e-mail messages. These messages will be used to train the antispam filter.

   Important

   Please make sure that the folder you choose contains no legitimate e-mail at all, otherwise the antispam performance will be considerably reduced.

   There are two advanced options under the directory list:
   - **Include all subfolders** - to include the subfolders to your selection.
   - **Automatically add to Spammers list** - to add the senders to the Spammers list. E-mail messages from these senders will always be marked as SPAM and processed accordingly.

6. **Summary**

   Here you can view all the settings for the configuration wizard. You can make any changes, by returning to the previous steps (click **Back**).

   If you do not want to make any modifications, click **Finish** to end the wizard.

13.3. Using the Antispam Toolbar in Your Mail Client Window

In the upper area of your mail client window you can see the Antispam toolbar. The Antispam toolbar helps you manage antispam protection directly from your mail client. You can easily correct Acronis Internet Security if it marked a legitimate message as SPAM.

Important

Acronis Internet Security integrates into the most commonly used mail clients through an easy-to-use antispam toolbar. For a complete list of supported mail clients, please refer to "*Supported E-mail Clients and Protocols*" (p. 67).

Each button from the Acronis Internet Security toolbar will be explained below:

- **Is Spam** - sends a message to the Bayesian module indicating that the selected e-mail is spam. The e-mail will be tagged as SPAM and moved to the **Spam** folder.

  The future e-mail messages that fit the same patterns will be tagged as SPAM.

- **Not Spam** - sends a message to the Bayesian module indicating that the selected e-mail is not spam and Acronis Internet Security should not have tagged it. The e-mail will be moved from the **Spam** folder to the **Inbox** directory.

  The future e-mail messages that fit the same patterns will no longer be tagged as SPAM.

  Important

  The **Not Spam** button becomes active when you select a message marked as SPAM by Acronis Internet Security (normally these messages are located in the **Spam** folder).

- **Add Spammer** - adds the sender of the selected e-mail to the Spammers list. You may need to click **OK** to acknowledge. The e-mail messages received from addresses in the Spammers list are automatically marked as `[spam]`.
- **Add Friend** - adds the sender of the selected e-mail to the Friends list. You may need to click **OK** to acknowledge. You will always receive e-mail messages from this address no matter what they contain.
- **Spammers** - opens the **Spammers list** that contains all the e-mail addresses from which you don't want to receive messages, regardless of their content. For more information, please refer to "*Configuring the Spammers List*" (p. 74).
- **Friends** - opens the **Friends list** that contains all the e-mail addresses from which you always want to receive e-mail messages, regardless of their content. For more information, please refer to "*Configuring the Friends List*" (p. 73).
- **Settings** - opens the **Settings** window where you can specify some options for the **Antispam** module.
- **Wizard** - opens the antispam optimization wizard. This wizard help you train the Bayesian filter in order to further increase the efficiency of your antispam protection. You can also add addresses from your Address Book to your Friends list / Spammers list.
- **Acronis Internet Security Antispam** - opens a window where you can configure the antispam protection level and the antispam filters.

13.3.1. Indicating Detection Errors

If you are using a supported mail client, you can easily correct the antispam filter (by indicating which e-mail messages should not have been marked as `[spam]`). Doing so will considerably improve the efficiency of the antispam filter. Follow these steps:

1. Open your mail client.
2. Go to the junk mail folder where spam messages are moved.

3. Select the legitimate message incorrectly marked as [spam] by Acronis Internet Security.
4. Click the **Add Friend** button on the Acronis Internet Security antispam toolbar to add the sender to the Friends list. You may need to click **OK** to acknowledge. You will always receive e-mail messages from this address no matter what they contain.
5. Click the **Not Spam** button on the Acronis Internet Security antispam toolbar (normally located in the upper part of the mail client window). This indicates to the Learning Engine that the selected message is not spam. The e-mail message will be moved to the Inbox folder. The next e-mail messages that fit the same patterns will no longer be marked as [spam].

13.3.2. Indicating Undetected Spam Messages

If you are using a supported mail client, you can easily indicate which e-mail messages should have been detected as spam. Doing so will considerably improve the efficiency of the antispam filter. Follow these steps:

1. Open your mail client.
2. Go to the Inbox folder.
3. Select the undetected spam messages.
4. Click the **Is Spam** button on the Acronis Internet Security antispam toolbar (normally located in the upper part of the mail client window). This indicates to the Learning Engine that the selected messages are spam. They are immediately marked as [spam] and moved to the junk mail folder. The next e-mail messages that fit the same patterns will be marked as [spam].

13.3.3. Retraining the Learning Engine (Bayesian)

If your antispam filter is very inaccurate, you may need to wipe the Bayesian database and retrain the Bayesian filter.

Before training the Learning Engine (Bayesian), prepare a folder containing only SPAM messages and another one containing only legitimate messages. The Learning Engine will analyze them and learn the characteristics that define the spam or legitimate messages that you usually receive. In order for the training to be efficient, there must be over 50 messages in each category.

To reset the Bayesian database and retrain the Learning Engine, follow these steps:

1. Open your mail client.
2. On the Acronis Internet Security antispam toolbar, click the **Wizard** button to start the antispam configuration wizard.
3. Click **Next**.

4. Select **Skip this step** and click **Next**.
5. Select **Clear antispam filter database** and click **Next**.
6. Select the folder containing legitimate messages and click **Next**.
7. Select the folder containing SPAM messages and click **Next**.
8. Click **Finish** to start the training process.
9. When training is completed, click **Close**.

13.3.4. Saving and Loading Bayesian Database

You can save the Bayesian database to a file so that you can use it with another Acronis Internet Security product or after reinstalling Acronis Internet Security.

Click the **Settings** button on the Acronis Internet Security antispam toolbar.

To save the Bayesian database, click the **Save Bayes** button and save it to the desired location. The file will have a `.dat` extension.

To load a previously saved Bayesian database, click the **Load Bayes** button and open the corresponding file.

13.3.5. Configuring General Settings

To configure general antispam settings for your mail client, click the **Settings** button on the Acronis Internet Security antispam toolbar.

The following options are available:

- **Move message to Deleted Items** - moves the spam messages to the **Deleted Items** (only for Microsoft Outlook Express / Windows Mail);
- **Mark spam e-mail messages as 'read'** - marks the spam messages as read automatically, so as not to be disturbing when they arrive.

Click the **Alerts** tab if you want to access the section where you can disable the apparition of the confirmation windows for the **Add spammer** and **Add friend** buttons.

In the **Alerts** window you can also enable/disable the apparition of the **Please select an email message** alert. This alert appears when you select a group instead of an email message.

13.4. Adjusting the Protection Level

Some of the antispam filters can identify spam e-mails directly, while others add a spam score to the e-mail, based on the spam characteristics detected.

The antispam protection level is used to determine if an e-mail message can be considered spam based on its total spam score (received after being checked by all of the antispam filters).

You should not change the antispam protection level, unless the antispam protection does not work as expected. However, rather than independently change the protection level, it is recommended that you first read *"Antispam Filter Does Not Work Properly" (p. 156)* and follow the instructions to correct the problem.

To adjust the antispam protection level:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antispam > Status**.
3. Drag the slider along the scale to set the appropriate protection level. To set the default protection level (**Moderate to Aggressive**) click **Default Level**.

Use the description on the right side of the scale to choose the protection level that better fits your security needs. The description also informs you about any additional actions you should take in order to avoid potential problems or to increase antispam detection efficiency.

13.5. Configuring the Friends List

The **Friends list** is a list of all the e-mail addresses from which you always want to receive messages, regardless of their content. Messages from your friends are not labeled as spam, even if the content resembles spam.

Note

Any mail coming from an address contained in the **Friends list**, will automatically be delivered to your Inbox without further processing.

To configure and manage the Friends list:

- If you are using Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, click the **Friends** button on the Acronis Internet Security antispam toolbar integrated into your mail client.
- Alternatively, follow these steps:
  1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
  2. Go to **Antispam > Status**.
  3. Click **Manage Friends**.

To add an e-mail address, select the **E-mail address** option, enter the address and click the button next to the edit field. Syntax: name@domain.com.

To add all the e-mail addresses from a specific domain, select the **Domain name** option, enter the domain name and click the button next to the edit field. Syntax:

- @domain.com, *domain.com and domain.com - all the received e-mail messages from domain.com will reach your **Inbox** regardless of their content;

- *domain* - all the received e-mail messages from domain (no matter the domain suffixes) will reach your **Inbox** regardless of their content;
- *com - all the received e-mail messages having the domain suffix com will reach your **Inbox** regardless of their content;

It is recommended to avoid adding entire domains, but this may be useful in some situations. For example, you can add the e-mail domain of the company you work for, or those of your trusted partners.

To delete an item from the list, select it and click the **Remove** button. To delete all entries from the list, click the **Clear list** button and then **Yes** to confirm.

You can save the Friends list to a file so that you can use it on another computer or after reinstalling the product. To save the Friends list, click the **Save** button and save it to the desired location. The file will have a `.bwl` extension.

To load a previously saved Friends list, click the **Load** button and open the corresponding `.bwl` file. To reset the content of the existing list when loading a previously saved list, select **Overwrite the current list**.

Click **Apply** and **OK** to save and close the **Friends list**.

13.6. Configuring the Spammers List

The **Spammers list** is a list of all the e-mail addresses from which you don't want to receive messages, regardless of their content. Any e-mail message received from an address contained in the **Spammers list** will be automatically marked as SPAM, without further processing.

To configure and manage the Spammers list:

- If you are using Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, click the **Spammers** button on the Acronis Internet Security antispam toolbar integrated into your mail client.
- Alternatively, follow these steps:
  1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
  2. Go to **Antispam > Status**.
  3. Click **Manage Spammers**.

To add an e-mail address, select the **E-mail address** option, enter the address and click the button next to the edit field. Syntax: name@domain.com.

To add all the e-mail addresses from a specific domain, select the **Domain name** option, enter the domain name and click the button next to the edit field. Syntax:

- @domain.com, *domain.com and domain.com - all the received e-mail messages from domain.com will be tagged as SPAM;
- *domain* - all the received e-mail messages from domain (no matter the domain suffixes) will be tagged as SPAM;

- *com - all the received e-mail messages having the domain suffix com will be tagged as SPAM.

It is recommended to avoid adding entire domains, but this may be useful in some situations.

Warning

Do not add domains of legitimate web-based e-mail services (such as Yahoo, Gmail, Hotmail or other) to the Spammers list. Otherwise, the e-mail messages received from any registered user of such a service will be detected as spam. If, for example, you add `yahoo.com` to the Spammers list, all e-mail messages coming from `yahoo.com` addresses will be marked as `[spam]`.

To delete an item from the list, select it and click the **Remove** button. To delete all entries from the list, click the **Clear list** button and then **Yes** to confirm.

You can save the Spammers list to a file so that you can use it on another computer or after reinstalling the product. To save the Spammers list, click the **Save** button and save it to the desired location. The file will have a `.bwl` extension.

To load a previously saved Spammers list, click the **Load** button and open the corresponding `.bwl` file. To reset the content of the existing list when loading a previously saved list, select **Overwrite the current list**.

Click **Apply** and **OK** to save and close the **Spammers list**.

13.7. Configuring the Antispam Filters and Settings

As described in "*Antispam Insights*" (p. 64), Acronis Internet Security uses a combination of different antispam filters to identify spam. The antispam filters are pre-configured for efficient protection.

You can disable each one of these filters or change their settings, but this is not recommended. These are some changes you may want to make:

- Depending on whether or not you receive legitimate e-mails written in Asian or Cyrillic characters, disable or enable the setting that automatically blocks such e-mails.

Note

The corresponding setting is disabled in the localized versions of the program that use such charsets (for example, in the Russian or Chinese version).

- If you do not want to automatically add the recipients of your sent mail to the Friends list, you can disable the corresponding setting. In this case, add your contacts to the Friends list, as described in "*Configuring the Friends List*" (p. 73).
- Advanced users can try to adjust the size of the Bayesian dictionary to achieve better antispam performance. A smaller number of words will result in faster, but

less precise, antispam processing. A larger number of words will increase antispam detection accuracy, but it will take more time to access your e-mails.

Note

It may take several adjustments of the Bayesian dictionary size to reach the desired performance level. If the result is not as expected, set back the default and recommended size of 200.000 words.

To configure the antispam settings and filters:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antispam > Settings**.
3. Configure the settings as needed. To find out what an option does, keep the mouse over it and read the description displayed at the bottom of the window.
4. Click **Apply** to save the changes.

To apply the default settings, click **Default**.

14. Parental Control

Acronis Internet Security Parental Control enables you to control the access to the Internet and to specific applications for each user holding a user account on the system.

You can configure Parental Control to block:

- inappropriate web pages.
- Internet access, for specific periods of time (such as when it's time for lessons).
- web pages, e-mail messages and instant messages if they contain specific keywords.
- applications like games, chat, filesharing programs or others.
- instant messages sent by IM contacts other than those allowed.

Important

Only users with administrative rights on the system (system administrators) can access and configure Parental Control. To make sure that only you can change the Parental Control settings for any user, you can protect them with a password. You will be prompted to configure the password when you enable the Parental Control for a specific user.

Once you have configured Parental Control, you can easily find out what your children are doing on the computer.

14.1. Configuring Parental Control

Before you configure Parental Control, create separate Windows user accounts for your children to use. This will allow you to know exactly what each of them is doing on the computer. You should create limited (standard) user accounts so that they cannot change the Parental Control settings. For more information, please refer to "*How Do I Create Windows User Accounts?*" (p. 147).

If your children can access an administrator account on their computer, you must configure a password to protect the Parental Control settings. For more information, please refer to "*Protecting Parental Control Settings*" (p. 79).

To configure Parental Control:

1. Make sure you are logged on to the computer with an administrator account. Only users with administrative rights on the system (system administrators) can access and configure Parental Control.
2. Open Acronis Internet Security.
3. Depending on the user interface view mode, access the Parental Control settings as follows:

Intermediate View

Go to the **Security** tab and click **Parental Control** in the Quick Tasks area on the left side of the window.

Expert View

Click **Parental Control** on the left-side menu.

Note

In Basic View and Intermediate View, you can configure a shortcut so that you can access these settings from your dashboard. For more information, please refer to "*My Tools*" (p. 16).

You can see information regarding the Parental Control status for each Windows user account. The age category is listed below each user name if Parental Control is enabled. If Parental Control is disabled, the status is **not configured**.

To configure Parental Control for a specific user account:

1. Use the switch to turn on Parental Control for that user account.
2. You will be prompted to set the Parental Control password. Set a password to protect your Parental Control settings. For more information, please refer to "*Protecting Parental Control Settings*" (p. 79).
3. Set the age category to allow your child to access only websites appropriate for his/her age. Setting the age of the child will automatically load settings considered appropriate for that age category, based on child development standards.
4. If you want to configure the Parental Control settings in detail, click **Settings**. Click a tab to configure the corresponding Parental Control feature:
   - **Web** - to filter web navigation according to the rules set by you in the Web section.
   - **Applications** - to block access to the applications specified by you in the Applications section.
   - **Keywords** - to filter web, mail and instant messaging access according to the rules set by you in the Keywords section.
   - **Messaging** - to allow or block chat with IM contacts according to the rules set by you in the Messaging section.

Note

To learn how to configure them, please refer to the following topics in this chapter.

Configure the monitoring options as needed:

- **Send me an activity report via e-mail.** An e-mail notification is sent every time Acronis Internet Security Parental Control blocks an activity. You must first configure the notification settings.
- **Save an internet traffic log.** Logs the websites visited by users for whom Parental Control is enabled.

For more information, please refer to "*Monitoring Children Activity*" (p. 84).

14.1.1. Protecting Parental Control Settings

If you are not the only person with administrative rights using this computer, it is recommended that you protect your Parental Control settings with a password. By setting a password, you will prevent other users with administrative rights from changing the Parental Control settings that you configured for a specific user.

Acronis Internet Security will ask you by default to set a password when enabling Parental Control. To set the password protection, do the following:

1. Type the password in the **Password** field.
2. Type the password again in the **Retype Password** field to confirm it.
3. Click **OK** to save the password and close the window.

Once you set the password, if you want to change the Parental Control settings, you will be asked to provide the password. The other system administrators (if any) will also have to provide this password in order to change the Parental Control settings.

Note

This password will not protect other Acronis Internet Security settings.

In case you do not set a password and you do not want this window to appear again, check **Don't ask for a password when enabling Parental Control**.

Important

If you forget the password, you will have to reinstall the program or to contact Acronis Internet Security for support.

To remove the password protection:

1. Open Acronis Internet Security and click the **Options** button in the upper-right corner of the window.
2. Go to **General Settings**.
3. Use the switch to turn off the **Settings password** option.
4. Enter the password.
5. Click **OK**.

14.1.2. Web Control

The **Web Control** helps you to block access to web sites with inappropriate content. A list of candidates for blocking both sites and parts thereof is provided and updated by Acronis Internet Security, as part of the regular update process.

Note
When you enable Parental Control and set the age of your child, Web Control is automatically enabled and configured to block access to websites considered to be inappropriate for your child's age.

To configure Web Control for a specific user account:

1. Access the Acronis Internet Security Parental Control settings window for that user account.
2. Click the **Web** tab.
3. Use the switch to turn on Web Control.
4. You can check what web categories are automatically blocked / restricted for the currently selected age group. If you are not satisfied with the default settings, you can configure them as needed.

   To change the action configured for a specific category of web content, click the current status and select the desired action from the menu.
5. If you want to, create your own rules to allow or block access to specific websites. If Parental Control automatically blocks access to a website, you can create a rule to explicitly allow access to that website.
6. You can set limits on how much time your child spends on the Internet. For more information, please refer to "Restricting Internet Access By Time" (p. 81).

Creating Web Control Rules

To allow or block access to a website, follow these steps:

1. Click **Allow Website** or **Block Website**.
2. Enter the website address in the **Website** field.
3. Select the desired action for this rule - **Allow** or **Block**.
4. Click **Finish** to add the rule.

Managing Web Control Rules

The Website Control rules that have been configured are listed in the table on the lower side of the window. The website address and current status are listed for each Web Control rule.

To delete a rule, select it and click **Remove**.

To edit a rule, select it and click **Edit** or double-click it. Make the necessary changes in the configuration window.

Restricting Internet Access By Time

In the Schedule Web Access section, you can set limits on how much time your child spends on the Internet.

To completely block access to the Internet, select **Block Web Access**.

To restrict Internet access to certain times of day:

1. Select **Time limit web access**.
2. Click **Change Schedule**.
3. Select from the grid the time intervals during which Internet access is blocked. You can click individual cells, or you can click and drag to cover longer periods.
4. Click **Save**.

Note
Acronis Internet Security will perform updates every hour no matter if web access is blocked.

14.1.3. Application Control

The **Applications Control** helps you to block any application from running. Games, media and messaging software, as well as other categories of software and malware can be blocked this way. Applications blocked in this manner are also protected from modifications, and cannot be copied or moved. You can block applications permanently or just during certain time intervals, such as those when your children should be doing their homework.

To configure Application Control for a specific user account:

1. Access the Acronis Internet Security Parental Control settings window for that user account.
2. Click the **Applications** tab.
3. Use the switch to turn on Application Control.
4. Create rules for the applications you want to block or restrict access to.

Creating Application Control Rules

To block or restrict access to an application, follow these steps:

1. Click **Block Application** or **Restrict Application**.
2. Click **Browse** to locate the application to which you want to block/restrict access. Installed applications are usually located in the `C:\Program Files` folder.

3. Select the action of the rule:
   - **Block permanently** to block access to the application completely.
   - **Block based on this schedule** to restrict access to certain time intervals.

   If you choose to restrict access rather than block the application completely, you must also select from the grid the days and the time intervals during which access is blocked.
4. Click **Save** to add the rule.

Managing Application Control Rules

The Application Control rules that have been configured are listed in the table on the lower side of the window. The name of the application, the path and the current status are listed for each Application Control rule.

To delete a rule, select it and click **Remove**.

To edit a rule, select it and click **Edit** or double-click it. Make the necessary changes in the configuration window.

14.1.4. Keywords Control

Keywords Control helps you block users' access to e-mail messages, web pages and instant messages that contain specific words. Using Keywords Control, you can prevent your children from seeing inappropriate words or phrases when they are online. Furthermore, you can ensure they will not be giving out personal information (such as the home address or phone number) to people they met on the Internet.

Note
The instant messaging Keywords Control is only available for Yahoo Messenger and Windows Live (MSN) Messenger.

To configure Keywords Control for a specific user account:

1. Access the Acronis Internet Security Parental Control settings window for that user account.
2. Click the **Keywords** tab.
3. Use the switch to turn on Keywords Control.
4. Create Keywords Control rules to prevent inappropriate words from being displayed or important information from being sent.

Creating Keywords Control Rules

To block a word or phrase, follow these steps:

1. Click **Block Keyword**.

2. Set Keyword Information.

   You must set the following parameters:

   - **Keyword category** - type the name of the rule in this field.
   - **Keyword** - type the word or phrase you want to block in the field. If you want only whole words to be detected, select the **Match whole words** check box.

3. Select the Filtering Type.

   - **Block viewing** - select this option for rules created to prevent inapropiate words from being displayed.
   - **Block sending** - select this option for rules created to prevent important information from being sent.

4. Select the traffic type Acronis Internet Security should scan for the specified word.

Option	Description
Web	Web pages that contain the keyword are blocked.
E-mail	E-mail messages that contain the keyword are blocked.
Instant Messaging	Instant messages that contain the keyword are blocked.

5. Click **Finish** to add the rule.

From now on, any attempt to send the specified data (through e-mail, instant messaging or over a web page) will fail. An alert message will be displayed indicating that Acronis Internet Security has blocked identity specific content from being sent.

Managing Keywords Control Rules

The Keywords Control rules that have been configured are listed in the table. Detailed information is provided for each rule.

To delete a rule, select it and click **Remove**.

To edit a rule, select it and click **Edit** or double-click it. Make the necessary changes in the configuration window.

14.1.5. Instant Messaging (IM) Control

The Instant Messaging (IM) Control allows you to specify the IM contacts your children are allowed to chat with.

Note

The IM Control is only available for Yahoo Messenger and Windows Live (MSN) Messenger.

To configure IM Control for a specific user account:

1. Access the Acronis Internet Security Parental Control settings window for that user account.
2. Click the **Messaging** tab.
3. Use the switch to turn on Instant Messaging Control.
4. Select the preferred filtering method and, depending on your choice, create appropriate rules.

   - **Allow IM with all contacts, except the ones in the list**

     In this case, you must specify the IM IDs to be blocked (people who your child should not talk to).

   - **Block IM with all contacts, except the ones in the list**

     In this case, you must specify the IM IDs your child is explicitly allowed to instant message with. For example, you can allow instant messaging with family members, friends from school or neighbours.

     This second option is recommended if your child is under 14 years old.

Creating Instant Messaging (IM) Control Rules

To allow or block instant messaging with a contact, follow these steps:

1. Click **Block IM ID** or **Allow IM ID**.
2. Type the e-mail address or the user name used by the IM contact in the **E-mail or IM ID** field.
3. Choose the IM program the contact associates with.
4. Select the desired action for this rule - **Allow** or **Block**.
5. Click **Finish** to add the rule.

Managing Instant Messaging (IM) Control Rules

The IM Control rules that have been configured are listed in the table on the lower side of the window.

To delete a rule, select it and click **Remove**.

To edit a rule, select it and click **Edit** or double-click it. Make the necessary changes in the configuration window.

14.2. Monitoring Children Activity

Acronis Internet Security helps you keep track of what your children are doing on the computer even when you are away.

By default, when Parental Control is enabled, your children's activities are logged. In this way, you can always find out exactly what websites they have visited, what applications they have used, what activities have been blocked by Parental Control etc.

You can also configure Acronis Internet Security to send you e-mail notifications when Parental Control blocks an activity.

14.2.1. Checking the Parental Control Logs

To check what your children have been doing recently on the computer, access the Parental Control logs. Follow these steps:

1. Open Acronis Internet Security.
2. Click the **View Logs** link in the bottom-right corner of the window.
3. Click **Parental Control** on the left-side menu.

Note

You can also open these logs from the Parental Control window by clicking **View Logs**.

If you do not share the computer with your children, you can configure the Acronis Internet Security home network so that you can access the Parental Control logs remotely (from your computer). For more information, please refer to *"Home Network" (p. 131)*.

The Parental Control logs provide detailed information about your children's computer and Internet activities. Information is organized under several tabs:

General

Provides general information about your children's recent activities, such as the most visited websites and the most used applications.

You can filter information by user and time period.

Application Log

Helps you find out what applications your children have been using recently.

Double-click the events in the list to see more details. To delete a log entry, right-click it and select **Delete**.

Internet Log

Helps you find out what websites your children have been visiting recently.

You can filter information by user and time period.

Other Events

Helps you find out detailed information about the Parental Control activity (for example, when Parental Control was enabled / disabled, what events have been blocked).

Double-click the events in the list to see more details. To delete a log entry, right-click it and select **Delete**.

14.2.2. Configuring E-mail Notifications

To receive e-mail notifications when Parental Control blocks an activity:

1. Open Acronis Internet Security.
2. Depending on the user interface view mode, access the Parental Control settings as follows:

   Intermediate View
   Go to the **Security** tab and click **Parental Control** in the Quick Tasks area on the left side of the window.

   Expert View
   Click **Parental Control** on the left-side menu.

   Note
   In Basic View and Intermediate View, you can configure a shortcut so that you can access these settings from your dashboard. For more information, please refer to "*My Tools*" (p. 16).

3. In the Settings section, select **Send me an activity report via e-mail**.
4. You will be prompted to configure your e-mail account settings. Click **Yes** to open the configuration window.

   Note
   You can open the configuration window later by clicking **Notifications Settings**.

5. Enter the e-mail address where the e-mail notifications are to be sent.
6. Configure the e-mail settings of the server used to send the e-mail notifications.

There are three options to configure the e-mail settings:

Use the current mail client settings
This option is selected by default when Acronis Internet Security manages to import the mail server settings from your mail client.

Click **Test Settings** to validate the settings. If any issues are found during validation, you will be informed what you have to do to correct them.

Select from one of the known servers
Select this option if you have an e-mail account with one of the web-based e-mail services in the list.

Click **Test Settings** to validate the settings. If any issues are found during validation, you will be informed what you have to do to correct them.

I want to configure the server settings myself

If you know the mail server settings, select this option and configure the settings as follows:

- **Outgoing SMTP Server** - type the address of the mail server used to send e-mail messages.
- If the server uses a different port than the default port 25, type it in the corresponding field.
- If the server requires authentication, select the **My SMTP server requires authentication** check box and type your user name and password in the corresponding fields.

Click **Test Settings** to validate the settings. If any issues are found during validation, you will be informed what you have to do to correct them.

Click **OK** to save the changes and close the window.

15. Privacy Control

Acronis Internet Security monitors dozens of potential "hotspots" in your system where spyware might act, and also checks any changes made to your system and software. It is effective in blocking Trojan horses and other tools installed by hackers, who try to compromise your privacy and send your personal information, like credit card numbers, from your computer to the hacker.

Privacy Control includes these components:

- Identity Control - helps you make sure that your personal information is not sent from your computer without your consent. It scans the e-mail and instant messages sent from your computer, as well as any data sent via web pages, and blocks any piece of information protected by the Identity Control rules you have created.
- Registry Control - asks for your permission whenever a program tries to modify a registry entry in order to be executed at Windows start-up.
- Cookie Control - asks for your permission whenever a new website tries to set a cookie.
- Script Control - asks for your permission whenever a website tries to activate a script or other active content.

By default, only Identity Control is enabled. You must configure appropriate Identity Control rules to prevent the unauthorized sending of confidential information. For more information, please refer to "*Configuring Identity Control*" (p. 90).

The other components of Privacy Control are interactive. If you enable them, you will be prompted, through alert windows, to allow or block specific actions when you browse new web sites or install new software. This is why they are usually used by advanced users.

15.1. Configuring Protection Level

The protection level helps you easily enable or disable the Privacy Control components.

To configure the protection level:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Privacy Control > Status**.
3. Make sure Privacy Control is enabled.
4. There are two options:
   - Drag the slider along the scale to set the appropriate protection level. Click **Default Level** to position the slider at the default level.

Use the description on the right side of the scale to choose the protection level that better fits your security needs.

- You can customize the protection level by clicking **Custom level**. In the window that will appear, select the protection controls you want to enable and click **OK**.

15.2. Identity Control

Identity Control protects you against the theft of sensitive data when you are online.

Consider a simple example: you have created an Identity Control rule that protects your credit card number. If a spyware software somehow manages to install on your computer, it cannot send your credit card number via e-mail, instant messages or web pages. Moreover, your children cannot use it to buy online or reveal it to people they met on the Internet.

To learn more, please refer to these topics:

- "*About Identity Control*" (p. 89).
- "*Configuring Identity Control*" (p. 90).
- "*Managing Rules*" (p. 92).

15.2.1. About Identity Control

Keeping confidential data safe is an important issue that bothers us all. Data theft has kept pace with the development of Internet communications and it makes use of new methods of fooling people into giving away private information.

Whether it is your e-mail or your credit card number, when they fall into the wrong hands such information may cause you damage: you may find yourself drowning in spam messages or you might be surprised to access an emptied account.

Identity Control protects you against the theft of sensitive data when you are online. Based on the rules you create, Identity Control scans the web, e-mail and instant messaging traffic leaving your computer for specific character strings (for example, your credit card number). If there is a match, the respective web page, e-mail or instant message is blocked.

You can create rules to protect any piece of information you might consider personal or confidential, from your phone number or e-mail address to your bank account information. Multiuser support is provided so that users logging on to different Windows user accounts can configure and use their own identity protection rules. If your Windows account is an administrator account, the rules you create can be configured to also apply when other users of the computer are logged on to their Windows user accounts.

Why use Identity Control?

- Identity Control is very effective in blocking keylogger spyware. This type of malicious applications records your keystrokes and sends them over the Internet to a malicious person (hacker). The hacker can find out sensitive information from the stolen data, such as bank account numbers and passwords, and use it to gain personal benefits.

  Supposing such an application manages to avoid antivirus detection, it cannot send the stolen data by e-mail, web or instant messages if you have created appropriate identity protection rules.

- Identity Control can protect you from phishing attempts (attempts to steal personal information). The most common phishing attempts make use of a deceiving e-mail to trick you into submitting personal information on a fake web page.

  For example, you may receive an e-mail claiming to be from your bank and requesting you to urgently update your bank account information. The e-mail provides you with a link to the web page where you must provide your personal information. Although they seem to be legitimate, the e-mail and the web page the misleading link directs you to are fake. If you click the link in the e-mail and submit your personal information on the fake web page, you will disclose this information to the malicious persons who organized the phishing attempt.

  If appropriate identity protection rules are in place, you cannot submit personal information (such as your credit card number) on a web page unless you have explicitly defined an exception for the respective web page.

- Using Identity Control rules, you can prevent your children from giving out personal information (such as the home address or phone number) to people they met on the Internet. Moreover, if you create rules to protect your credit card, they cannot use it to buy things online without your consent.

15.2.2. Configuring Identity Control

If you want to use Identity Control, follow these steps:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Privacy Control > Identity**.
3. Make sure Identity Control is enabled.

   Note
   If the option cannot be configured, go to the **Status** tab and enable Privacy Control.

4. Create rules to protect your sensitive data. For more information, please refer to "*Creating Identity Protection Rules*" (p. 91).

5. If needed, define specific exclusions from the rules you have created. For example, if you have created a rule to protect your credit card number, add the web sites where you usually use your credit card to the exclusions list. For more information, please refer to "*Defining Exclusions*" (p. 92).

Creating Identity Protection Rules

To create an identity protection rule, click the **Add** button and follow the configuration wizard. You can navigate through the wizard using the **Next** and **Back** buttons. To exit the wizard, click **Cancel**.

1. **Welcome Window**
2. **Set Rule Type and Data**

   You must set the following parameters:

   - **Rule Name** - type the name of the rule in this edit field.
   - **Rule Type** - choose the rule type (address, name, credit card, PIN, SSN etc).
   - **Rule Data** - type the data you want to protect in this edit field. For example, if you want to protect your credit card number, type all or part of it here.

     Important

     If you enter less than three characters, you will be prompted to validate the data. We recommend you to enter at least three characters in order to avoid the mistaken blocking of messages and web pages.

   All of the data you enter is encrypted. For extra safety, do not enter all of the data you wish to protect.
3. **Select Traffic Types and Users**

   a. Select the type of traffic you want Acronis Internet Security to scan.

   - **Scan Web (HTTP traffic)** - scans the HTTP (web) traffic and blocks the outgoing data that matches the rule data.
   - **Scan e-mail (SMTP traffic)** - scans the SMTP (mail) traffic and blocks the outgoing e-mail messages that contain the rule data.
   - **Scan IM (Instant Messaging) traffic** - scans the Instant Messaging traffic and blocks the outgoing chat messages that contain the rule data.

   You can choose to apply the rule only if the rule data matches whole words or if the rule data and the detected string case match.

   b. Specify the users for which the rule applies.

   - **Only for me (current user)** - the rule will apply only to your user account.
   - **Limited user accounts** - the rule will apply to you and all limited Windows accounts.

- **All users** - the rule will apply to all Windows accounts.

4. **Describe Rule**

   Enter a short description of the rule in the edit field. Since the blocked data (character string) is not displayed in plain text when accessing the rule, the description should help you easily identify it.

   Click **Finish**. The rule will appear in the table.

From now on, any attempt to send the specified data (through e-mail, instant messaging or over a web page) will fail. An alert message will be displayed indicating that Acronis Internet Security has blocked identity specific content from being sent.

Defining Exclusions

There are cases when you need to define exceptions to specific identity rules. Let's consider the case when you create a rule that prevents your credit card number from being sent over HTTP (web). Whenever your credit card number is submitted on a website from your user account, the respective page is blocked. If you want, for example, to buy footwear from an online shop (which you know to be secure), you will have to specify an exception to the respective rule.

To open the window where you can manage exceptions, click **Exclusions**.

To add an exception, follow these steps:

1. Click the **Add** button to add a new entry in the table.
2. Double-click **Specify excluded item** and provide the web site, the e-mail address or the IM contact that you want to add as exception.
3. Double-click **Traffic type** and choose from the menu the option corresponding to the type of address previously provided.
   - If you have specified a web address, select **HTTP**.
   - If you have specified an e-mail address, select **E-mail (SMTP)**.
   - If you have specified an IM contact, select **IM**.

To remove an exception from the list, select it and click the **Remove** button.

Click **OK** to save the changes.

15.2.3. Managing Rules

To manage the Identity Control rules:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Privacy Control > Identity**.

You can see the rules created so far listed in the table.

To delete a rule, select it and click the **Delete** button.

To edit a rule select it and click the **Edit** button or double-click it. A new window will appear. Here you can change the name, description and parameters of the rule (type, data and traffic). Click **OK** to save the changes.

15.3. Registry Control

A very important part of the Windows operating system is called the **Registry**. This is where Windows keeps its settings, installed programs, user information and so on.

The **Registry** is also used to define which programs should be launched automatically when Windows is started. Viruses often use this in order to be automatically launched when the user restarts his computer.

Registry Control keeps an eye on the Windows Registry - this is again useful for detecting Trojan horses. It will alert you whenever a program will try to modify a registry entry in order to be executed at Windows start-up. For more information, please refer to "*Registry Alerts*" (p. 22).

To configure Registry Control:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Privacy Control > Registry**.
3. Select the corresponding check box to enable Registry Control.

Note
If the option cannot be configured, go to the **Status** tab and enable Privacy Control.

Managing Rules

To delete a rule, select it and click the **Delete** button.

15.4. Cookie Control

Cookies are a very common occurrence on the Internet. They are small files stored on your computer. Websites create these cookies in order to keep track of specific information about you.

Cookies are generally made to make your life easier. For example they can help the website remember your name and preferences, so that you don't have to enter them on every visit.

But cookies can also be used to compromise your privacy, by tracking your surfing patterns.

This is where Cookie Control helps. When enabled, Cookie Control will prompt you for permission whenever a new web site tries to set or request a cookie. For more information, please refer to "*Cookie Alerts*" (p. 23).

To configure Cookie Control:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Privacy Control > Cookie**.
3. Select the corresponding check box to enable Cookie Control.

Note
If the option cannot be configured, go to the **Status** tab and enable Privacy Control.

4. You can configure rules for the web sites you visit regularly, but it is not really necessary. Rules are automatically created through the alert window, based on your answer.

Note
Because of the great number of cookies used on the Internet today, **Cookie Control** can be quite bothersome to begin with. At first, it will ask a lot of questions about sites trying to place cookies on your computer. As soon as you add your regular sites to the rule-list, surfing will become as easy as before.

Creating Rules Manually

To manually create a rule, click the **Add** button and configure the rule parameters in the configuration window. You can set the parameters:

- **Domain address** - type in the domain on which the rule should apply.
- **Action** - select the action of the rule.

Action	Description
Allow	The cookies on that domain will execute.
Deny	The cookies on that domain will not execute.

- **Direction** - select the traffic direction.

Type	Description
Outgoing	The rule applies only for the cookies that are sent out back to the connected site.
Incoming	The rule applies only for the cookies that are received from the connected site.

Type	Description
Both	The rule applies in both directions.

Note
You can accept cookies but never return them by setting the action to **Deny** and the direction to **Outgoing**.

Click **Finish**.

Managing Rules

To delete a rule, select it and click the **Delete** button. To modify the rule parameters, select the rule and click the **Edit** button or double-click it. Make the desired changes in the configuration window.

15.5. Script Control

Scripts and other codes such as ActiveX controls and Java applets, which are used to create interactive web pages, can be programmed to have harmful effects. ActiveX elements, for example, can gain total access to your data and they can read data from your computer, delete information, capture passwords and intercept messages while you're online. You should only accept active content from sites you fully know and trust.

If you enable Script Control, you will be prompted for permission whenever a new web site tries to run a script or other active content. For more information, please refer to "*Script Alerts*" (p. 22).

To configure Script Control:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Privacy Control > Script**.
3. Select the corresponding check box to enable Script Control.

Note
If the option cannot be configured, go to the **Status** tab and enable Privacy Control.

4. You can configure rules for the web sites you visit regularly, but it is not really necessary. Rules are automatically created through the alert window, based on your answer.

Creating Rules Manually

To manually create a rule, click the **Add** button and configure the rule parameters in the configuration window. You can set the parameters:

- **Domain address** - type in the domain on which the rule should apply.
- **Action** - select the action of the rule.

Action	Description
Allow	The scripts on that domain will execute.
Deny	The scripts on that domain will not execute.

Click **Finish**.

Managing Rules

To delete a rule, select it and click the **Delete** button. To modify the rule parameters, select the rule and click the **Edit** button or double-click it. Make the desired changes in the configuration window.

16. Firewall

The Firewall protects your computer from inbound and outbound unauthorized connection attempts. It is quite similar to a guard at your gate - it will keep a watchful eye on your Internet connection and keep track of who to allow access to the Internet and who to block.

Note
A firewall is essential if you have a broadband or DSL connection.

In Stealth Mode your computer is “hidden” from malicious software and hackers. The firewall module is capable of automatically detecting and protecting against port scans (streams of packets sent to a machine in order to find “access points”, often in preparation for an attack).

16.1. Protection Settings

To enable/disable and configure firewall protection, open Acronis Internet Security and, depending on the user interface view mode, proceed as follows:

Intermediate View
Go to the **Security** tab and click **Configure Firewall** in the Quick Tasks area on the left side of the window. Select the **Settings** tab in the new window that appears.

Expert View
Go to **Firewall > Settings**.

Important
To be protected against Internet attacks keep the **Firewall** enabled.

At the top of the section, you can see various statistics regarding detected activity.

At the bottom of the section you can see the Acronis Internet Security statistics regarding incoming and outgoing traffic. The graph shows the Internet traffic volume over the last two minutes.

Note
The graph is displayed only in Expert View.

16.1.1. Setting the Default Action

By default, Acronis Internet Security automatically allows all known programs from its white list to access network services and the Internet. For all the other programs, Acronis Internet Security prompts you through an alert window to specify the action

to be taken. The action you specify is applied every time the respective application requests network/Internet access.

Note

To view the Acronis Internet Security white list, click the corresponding button located in the **Settings** tab in Expert View or the **Programs** tab in Intermediate View.

You can drag the slider along the scale to set the default action to be taken on the applications requiring network/Internet access.

- Allow All
- Allow Known Programs
- Report
- Deny All

When you select an action a brief explanation is displayed for it.

16.1.2. Configuring Advanced Firewall Settings

In Expert View, you can configure the advanced firewall settings by clicking **Advanced Settings**.

The following options are available:

- **Enable Internet Connection Sharing(ICS) support** - enables support for Internet Connection Sharing(ICS).

  Note

  This option does not automatically enable ICS on your system, but only allows this type of connection in case you enable it from your operating system.

- **Detect applications that changed since the firewall rule has been created** - checks each application attempting to connect to the Internet to see if it has been changed since the rule controlling its access was added. If the application has been changed, an alert will prompt you to allow or to block the access of the application to the Internet.

  Note

  Applications might be changed by malware. We recommend you to keep this option selected and to allow access only to those applications that you expect to have changed after the rule controlling their access was created.

  Signed applications are supposed to be trusted and have a higher degree of security. You can check **Don't detect changes in digitally signed applications** in order to allow changed signed applications to connect to the Internet without your receiving an alert about this event.

- **Show Wi-Fi Notifications** - if you are connected to a wireless network, displays informative windows regarding specific network events (for example, when a new computer has joined the network).
- **Block port scans** - detects and blocks attempts to find out which ports are open.

  Port scans are frequently used by hackers to find out which ports are open on your computer. They might then break into your computer if they find a less secure or vulnerable port.
- **Enable strict automatic rules** - creates strict rules using the firewall alert window. With this option selected, Acronis Internet Security will prompt you for action and create rules for each different process that opens the application requesting network or Internet access.

16.2. Application Access Rules

To manage the firewall rules controlling applications' access to network resources and Internet, open Acronis Internet Security and, depending on the user interface view mode, proceed as follows:

Intermediate View
: Go to the **Security** tab and click **Configure Firewall** in the Quick Tasks area on the left side of the window. Select the **Programs** tab in the new window that appears.

Expert View
: Go to **Firewall > Programs**.

Intermediate View gives you access to basic configuration settings. To have more customization options, use Expert View.

16.2.1. Viewing Current Rules

You can see the programs (processes) for which firewall rules have been created in the table.

In Expert View, you can learn detailed information about each rule, as indicated by the table columns. To see the rules created for a specific application, click the + box next to the respective application. Clear the **Hide system rules** check box if you want to also see the rules regarding the system or the Acronis Internet Security processes.

- **Process/Network Types** - the process and the network adapter types the rule applies to. Rules are automatically created to filter network or Internet access through any adapter. You can manually create rules or edit existing rules to filter an application's network or Internet access through a specific adapter (for example, a wireless network adapter).

- **Command Line** - the command used to start the process in the Windows command line interface (**cmd**).
- **Protocol** - the IP protocol the rule applies to. You may see one of the following:

Protocol	Description
Any	Includes all IP protocols.
TCP	Transmission Control Protocol - TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.
UDP	User Datagram Protocol - UDP is an IP-based transport designed for high performance. Games and other video-based applications often use UDP.
A number	Represents a specific IP protocol (other than TCP and UDP). You can find the complete list of assigned IP protocol numbers at www.iana.org/assignments/protocol-numbers.

- **Network Events** - the network events the rule applies to. The following events may be taken into account:

Event	Description
Connect	Preliminary exchange of standard messages used by connection-oriented protocols (such as TCP) to establish a connection. With connection-oriented protocols, data traffic between two computers occurs only after a connection is established.
Traffic	Flow of data between two computers.
Listen	State in which an application monitors the network awaiting to establish a connection or to receive information from a peer application.

- **Local Ports** - the ports on your computer the rule applies to.
- **Remote Ports** - the ports on the remote computers the rule applies to.
- **Local** - whether the rule applies only to computers in the local network.
- **Action** - whether the application is allowed or denied access to network or Internet under the specified circumstances.

16.2.2. Adding Rules Automatically

With **Firewall** enabled, Acronis Internet Security monitors all applications and automatically creates a rule whenever an application tries to connect to the Internet. Depending on the application and the Acronis Internet Security firewall settings, this is done with or without your intervention.

If you are using Basic View or Intermediate View, connection attempts coming from unknown applications will be automatically blocked.

If you are using Expert View, you will be prompted for action, through an alert window, whenever an unknown application tries to connect to the Internet.

You can see the following: the application that is trying to access the Internet, the path to the application file, the destination, the protocol used and the port on which the application is trying to connect.

Click **Allow** to allow all traffic (inbound and outbound) generated by this application from the local host to any destination, over the respective IP protocol and on all ports. If you click **Block**, the application will be denied access to the Internet over the respective IP protocol completely.

Important
Allow inbound connection attempts only from IPs or domains you are sure to trust.

Based on your answer, a rule will be created, applied and listed in the table. The next time the application tries to connect, this rule will be applied by default.

16.2.3. Adding Rules Manually

Creating rules manually differs depending on the user interface view mode you use.

Intermediate View

1. Click **Browse** under **Add New Program**.
2. Locate the program for which you want to create a rule and click **Open**.
3. Click **Add rule**.

   Notice that the rule is now displayed in the table.
4. Select an action from the **Action** column: allow or deny access.

   The action will be applied to all rule parameters.

Expert View

1. Click the **Add rule** button. The configuration window will appear.
2. Configure the main and the advanced parameters as needed.
3. Click **OK** to add the new rule.

Rules can be modified only when configuring the firewall in Expert View. To modify an existing rule, follow these steps:

1. Click the **Edit rule** button or double-click the rule. The configuration window will appear.
2. Configure the main and the advanced parameters as needed.
3. Click **OK** to save the changes.

Configuring Main Parameters

The **Main** tab of the configuration window allows configuring the main rule parameters.

You can configure the following parameters:

- **Program Path.** Click **Browse** and select the application the rule applies to. If you want the rule to apply to all applications, select **Any**.
- **Command line.** If you want the rule to apply only when the selected application is opened with a specific command in the Windows command line interface, clear the **Any** check box and type the respective command in the edit field.
- **Protocol.** Select from the menu the IP protocol the rule applies to.
  - ▶ If you want the rule to apply to all protocols, select **Any**.
  - ▶ If you want the rule to apply to TCP, select **TCP**.
  - ▶ If you want the rule to apply to UDP, select **UDP**.
  - ▶ If you want the rule to apply to a specific protocol, select **Other**. An edit field will appear. Type the number assigned to the protocol you want to filter in the edit field.

Note

IP protocol numbers are assigned by the Internet Assigned Numbers Authority (IANA). You can find the complete list of assigned IP protocol numbers at www.iana.org/assignments/protocol-numbers.

- **Events.** Depending on the selected protocol, choose the network events the rule applies to. The following events may be taken into account:

Event	Description
Connect	Preliminary exchange of standard messages used by connection-oriented protocols (such as TCP) to establish a connection. With connection-oriented protocols, data traffic between two computers occurs only after a connection is established.

Event	Description
Traffic	Flow of data between two computers.
Listen	State in which an application monitors the network awaiting to establish a connection or to receive information from a peer application.

- **Adapter Types.** Select the adapter types the rule applies to.
- **Action.** Select one of the available actions:

Action	Description
Allow	The specified application will be allowed network / Internet access under the specified circumstances.
Deny	The specified application will be denied network / Internet access under the specified circumstances.

Configuring Advanced Parameters

The **Advanced** tab of the configuration window allows configuring advanced rule parameters.

You can configure the following advanced parameters:

- **Direction.** Select from the menu the traffic direction the rule applies to.

Direction	Description
Outbound	The rule applies only for the outgoing traffic.
Inbound	The rule applies only for the incoming traffic.
Both	The rule applies in both directions.

- **IP version.** Select from the menu the IP version (IPv4, IPv6 or any) the rule applies to.
- **Local Address.** Specify the local IP address and port the rule applies to as follows:
  - ▶ If you have more than one network adapters, you can clear the **Any** check box and type a specific IP address.
  - ▶ If you have selected TCP or UDP as protocol you can set a specific port or a range between 0 and 65535. If you want the rule to apply to all ports, select **Any**.

- **Remote Address.** Specify the remote IP address and port the rule applies to as follows:
  - ▶ To filter traffic between your computer and a specific computer, clear the **Any** check box and type its IP address.
  - ▶ If you have selected TCP or UDP as protocol you can set a specific port or a range between 0 and 65535. If you want the rule to apply to all ports, select **Any**.
- **Apply this rule only to directly connected computers.** Select this option when you want the rule to apply only to the local traffic attempts.
- **Check process parent chain for the original event.** You can only modify this parameter if you have selected **Strict automatic rules** (go to the Settings tab and click **Advanced Settings**). Strict rules mean that Acronis Internet Security prompts you for action when an application request network/Internet access every time the parent process is different.

16.2.4. Advanced Rule Management

If you need to see and edit the rules controlling applications in detail, click the **Advanced** button available when configuring the firewall in Expert View.

You can see the firewall rules listed by the order they are checked in. The table columns provide comprehensive information about each rule.

Note

When a connection attempt is made (whether incoming or outgoing), Acronis Internet Security applies the action of the first rule matching the respective connection. Therefore, the order by which rules are checked is very important.

To delete a rule, select it and click the **Delete Rule** button.

To edit an existing rule, select it and click the **Edit Rule** button or double-click it.

You can increase or decrease the priority of a rule. Click the **Move Up In List** button to increase the priority of the selected rule by one level, or click the **Move Down In List** button to decrease the priority of the selected rule by one level. To assign a rule the highest priority, click the **Move First** button. To assign a rule the lowest priority, click the **Move Last** button.

Click **Close** to close the window.

16.2.5. Deleting and Reseting Rules

Deleting and reseting rules is possible only when configuring the firewall in Expert View.

To delete a rule, select it and click the **Remove rule** button. You can select and delete several rules at once.

If you want to delete all the rules created for a specific application, select the application from the list and click the **Remove rule** button.

If you want to load the default rule set for the selected trust level, click **Reset Rules**.

16.3. Network Settings

To configure the network connection settings, open Acronis Internet Security and, depending on the user interface view mode, proceed as follows:

Intermediate View
: Go to the **Security** tab and click **Configure Firewall** in the Quick Tasks area on the left side of the window. Select the **Network** tab in the new window that appears.

Expert View
: Go to **Firewall > Network**.

The columns in the **Network Configuration** table provide detailed information on the network you are connected to and allow you to configure the connection settings:

- **Adapter** - the network adapter your computer uses to connect to the network or the Internet.
- **Network Type** - the type of network the adapter connects to. Depending on the network adapter configuration, Acronis Internet Security may automatically select a network type or prompt you for more information.

  Change the type by clicking the arrow from the **Network Type** column and selecting one of the available types from the list.

Network Type	Description
Trusted (Allow All)	Disable the firewall for the respective adapter.
Home/Office	Allow all traffic between your computer and computers in the local network.
Public	All traffic is filtered.
Untrusted (Block All)	Completely block network and Internet traffic through the respective adapter.

- **VPN** - whether the connection is a VPN.

Traffic going through VPN connections is filtered differently than traffic going through other network connections. If the connection is a VPN, click the arrow from the **VPN** column and select **Yes**.

In Expert View, two additional columns are displayed:

- **Stealth Mode** - whether you can be detected by other computers.

  To configure the Stealth Mode, click the arrow from the **Stealth Mode** column and select the desired option.

Stealth option	Description
On	Stealth Mode is on. Your computer is not visible from both the local network and the Internet.
Off	Stealth Mode is off. Anyone from the local network or the Internet can ping and detect your computer.
Remote	Your computer cannot be detected from the Internet. Local network users can ping and detect your computer.

- **Generic** - whether generic rules are applied to this connection.

  If the IP address of a network adapter is changed, Acronis Internet Security modifies the network type accordingly. If you want to keep the same type, click the arrow from the **Generic** column and select **Yes**.

16.3.1. Network Zones

You can add allowed or blocked computers for a specific adapter.

A trusted zone is a computer that you fully trust. All traffic between your computer and a trusted computer is allowed. To share resources with specific computers in an unsecured wireless network, add them as allowed computers.

A blocked zone is a computer that you do not want to communicate at all with your computer.

The **Network Zones** table displays the current network zones per adapter.

To add a zone, select the adapter and click **Add Zone**. A new window will appear.

Proceed as follows:

1. Select the IP address of the computer you want to add.
2. Select the action:
   - **Allow** - to allow all traffic between your computer and the selected computer.
   - **Deny** - to block all traffic between your computer and the selected computer.

3. Click **OK**.

16.4. Devices

To manage devices connected to the network, open Acronis Internet Security and, depending on the user interface view mode, proceed as follows:

Intermediate View
Go to the **Security** tab and click **Configure Firewall** in the Quick Tasks area on the left side of the window. Select the **Devices** tab in the new window that appears.

Expert View
Go to **Firewall > Devices**.

The printers, faxes and scanners detected in the network and the default actions set for them are listed in the table. To change the status of a device, double-click it in the table and select an action in the window that appears: allow or block communication with the device.

Use the provided buttons to manage the device list:

- **Add** - add a device which does not appear in the list.
- **Remove** - remove a selected device from the list.
- **Refresh Devices** - initiate a new scan of the network to update the device list.

16.5. Connection Control

To monitor the current network / Internet activity (over TCP and UDP) sorted by application and to open the Acronis Internet Security Firewall log, follow these steps:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Firewall > Activity**.

You can see the total traffic sorted by application. For each application, you can see the connections and the open ports, as well as statistics regarding the outgoing & incoming traffic speed and the total amount of data sent / received.

If you want to see the inactive processes too, clear the **Hide inactive processes** check box.

The meaning of the icons is as follows:

- Indicates an outgoing connection.
- Indicates an incoming connection.
- Indicates an open port on your computer.

The window presents the current network / Internet activity in real-time. As connections or ports are closed, you can see that the corresponding statistics are dimmed and that, eventually, they disappear. The same thing happens to all statistics corresponding to an application which generates traffic or has open ports and which you close.

For a comprehensive list of events regarding the Firewall module usage (enabling/disabling firewall, traffic blocking, modifying settings) or generated by the activities detected by this module (scanning ports, blocking connection attempts or traffic according to the rules) view the Acronis Internet Security Firewall log file by clicking **Show Log**. The file is located in the Common Files folder of the current Windows user, under the path: `...Acronis Internet Security\Acronis Internet Security Firewall\bdfirewall.txt`.

If you want the log to contain more information, select **Increase log verbosity**.

16.6. Troubleshooting Firewall

In case you experience an issue you suspect is caused by the Acronis Internet Security Firewall, a Troubleshoot Wizard is available to help you solve it.

To start the wizard, open Acronis Internet Security and, depending on the user interface view mode, proceed as follows:

Intermediate View
: Go to the **Security** tab and click **Configure Firewall** in the Quick Tasks area on the left side of the window. Select the **Settings** tab in the new window that appears and click **Troubleshoot**.

Expert View
: Go to **Firewall > Settings** and click **Troubleshoot**.

The wizard can help you quickly solve the following connectivity problems commonly associated with the firewall configuration:

- I am trying to print and the action fails.
- I am trying to access a computer in my network and the action fails.
- I am trying to access the Internet and the action fails.

If none of the situations describes the problem you are experiencing, select **Other Firewall Problem** to open the **Support Tool** window.

For more information on this wizard, please refer to the Troubleshooting section of this guide

17. Vulnerability

An important step in protecting your computer against malicious persons and applications is to keep up to date the operating system and the applications you regularly use. Moreover, to prevent unauthorized physical access to your computer, strong passwords (passwords that cannot be easily guessed) must be configured for each Windows user account.

Acronis Internet Security regularly checks your system for vulnerabilities and notifies you about the existing issues.

17.1. Checking for Vulnerabilities

You can check for vulnerabilities and fix them step by step by using the **Vulnerability Scan** wizard. To start the wizard, open Acronis Internet Security and, depending on the user interface view mode, proceed as follows:

Intermediate View
: Go to the **Security** tab and click **Vulnerability Scan** in the Quick Tasks area on the left side of the window.

Expert View
: Go to **Vulnerability > Status** and click **Check Now**.

Follow the six-step guided procedure to remove vulnerabilities from your system. You can navigate through the wizard using the **Next** button. To exit the wizard, click **Cancel**.

1. **Protect your PC**

   Select vulnerabilities to check.

2. **Check for Issues**

   Wait for Acronis Internet Security to finish checking your system for vulnerabilities.

3. **Windows Updates**

   You can see the list of critical and non-critical Windows updates that are not currently installed on your computer. Select the updates you want to install.

4. **Application Updates**

   If an application is not up to date, click the provided link to download the latest version.

5. **Weak Passwords**

   You can see the list of the Windows user accounts configured on your computer and the level of protection their password provides. Click **Fix** to modify the weak passwords.

6. **Summary**

This is where you can view the operation result.

17.2. Status

To see the current vulnerability status and enable/disable automatic vulnerability scanning, follow these steps:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Vulnerability > Status**.

The table displays the issues covered in the last vulnerability check and their status. You can see the action you have to take to fix each vulnerability, if any. If the action is **None**, then the respective issue does not represent a vulnerability.

Important

To be automatically notified about system or application vulnerabilities, keep the **Automatic Vulnerability Scanning** enabled.

Depending on the issue, to fix a specific vulnerability proceed as follows:

- If Windows updates are available, click **Install** in the **Action** column to install them.
- If an application is outdated, click **More info** to view version information and find a link to the vendor web page from where you can install the latest version of that application.
- If a Windows user account has a weak password, click **View & Fix** to force the user to change the password at the next logon or change the password yourself. For a strong password, use a combination of uppercase and lowercase letters, numbers and special characters (such as #, $ or @).
- If the Media Autorun feature is enabled in Windows, click **Fix** to disable it.

17.3. Settings

To configure the settings of the automatic vulnerability checking, follow these steps:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Vulnerability > Settings**.
3. Select the check boxes corresponding to the system vulnerabilities you want to be regularly checked.
   - **Critical Windows Updates**
   - **Regular Windows Updates**
   - **Application Updates**
   - **Weak Passwords**

- **Media Autorun**

Note

If you clear the check box corresponding to a specific vulnerability, Acronis Internet Security will no longer notify you about the related issues.

18. Chat Encryption

The contents of your instant messages should remain between you and your chat partner. By encrypting your conversations, you can make sure anyone trying to intercept them on their way to and from your contacts will not be able to read their contents.

By default, Acronis Internet Security encrypts all your instant messaging chat sessions provided that:

- Your chat partner has a Acronis Internet Security product installed that supports Chat Encryption and Chat Encryption is enabled for the instant messaging application used for chatting.
- You and your chat partner use either Yahoo Messenger or Windows Live (MSN) Messenger.

Important
Acronis Internet Security will not encrypt a conversation if a chat partner uses a web-based chat application such as Meebo, or if one of the chat partners uses Yahoo! and the other Windows Live (MSN).

To configure instant messaging encryption:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Encryption > Chat Encryption**.

Note
You can easily configure instant messaging encryption for each chat partner using the Acronis Internet Security toolbar in the chat window.

By default, Chat Encryption is enabled for both Yahoo Messenger and Windows Live (MSN) Messenger. You can choose to disable Chat Encryption for a specific chat application only or completely.

Two tables are displayed:

- **Do not encrypt conversations with** - lists the user IDs and the associated instant messaging program for which encryption is disabled. To remove a contact from the list, select it and click the **Remove** button.
- **All Current Connections** - lists the current instant messaging connections (user ID and associated IM program) and whether or not they are encrypted. A connection may not be encrypted for these reasons:
  - ▶ You explicitly disabled encryption for the respective contact.

▶ Your contact does not have installed a Acronis Internet Security product that supports Chat Encryption.

18.1. Disabling Encryption for Specific Users

To disable encryption for a specific user, follow these steps:

1. Click the **Add** button to open the configuration window.
2. Type in the edit field the user ID of your contact.
3. Select the instant messaging application associated with the contact.
4. Click **OK**.

18.2. Acronis Internet Security Toolbar in the Chat Window

You can easily configure instant messaging encryption using the Acronis Internet Security toolbar from the chat window.

The toolbar should be located in the bottom-right corner of the chat window. Look for the Acronis Internet Security logo to find it.

Note

The toolbar indicates that a conversation is encrypted by displaying a small key next to the Acronis Internet Security logo.

By clicking the Acronis Internet Security toolbar you are provided with the following options:

- **Permanently disable encryption for `contact`.**
- **Invite `contact` to use encryption.** To encrypt your conversations, your contact must install Acronis Internet Security and use a compatible IM program.
- **Add `contact` to Parental Control blacklist.** If you add the contact to the Parental Control blacklist and Parental Control is enabled, you will no longer see the instant messages sent by that contact. To remove the contact from the blacklist, click the toolbar and select **Remove `contact` from Parental Control blacklist**.

19. File Encryption

Acronis Internet Security File Encryption enables you to create encrypted, password-protected logical drives (or vaults) on your computer where you can securely store your confidential and sensitive documents. The data stored on the vaults can only be accessed by users who know the password.

The password allows you to open, store data on and close a vault while maintaining its security. While a vault is open, you can add new files, access current files or change them.

Physically, the vault is a file stored on the local hard drive having the `.bvd` extension. Although the physical files representing the vaulted drives can be accessed from a different operating system (such as Linux), the information stored on them cannot be read because it is encrypted.

File Encryption is enabled by default. To disable it, follow these steps:

1. Right-click the Acronis Internet Security icon in the system tray and select **Preferences**.
2. In the Preferences window that appears, click the switch corresponding to **File Encryption**.

If you disable File Encryption, all file vaults will be locked and you will no longer be able to access the files they contain.

File vaults can be managed from the Acronis Internet Security window or by using the Windows contextual menu and logical drive associated with the vault.

19.1. Managing File Vaults From the Acronis Internet Security Interface

The way in which you can access and manage your file vaults differs depending on the interface view mode you use. The following section detail how you can manage file vaults.

19.1.1. Create Vault

To create a new vault, open Acronis Internet Security and, depending on the user interface view mode, proceed as follows:

Intermediate View

Go to **File Storage** and click **Create File Vault** in the File Encryption area.

Expert View

Go to **Encryption > File Encryption** in Expert View and do one of the following:

- Click **Choose Action** above the file vaults table and select **Create File Vault** from the menu.

- Right-click in the vaults table and select **Create File Vault**.

A new window will appear.

1. Specify the location and the name of the vault file.
   - Click **Browse**, select the location of the vault and save the vault file under the desired name.
   - Type the name and the path of the vault file on the disk in the corresponding fields .
2. Choose a drive letter from the menu. When you open the vault, a virtual disk drive labeled with the selected letter appears in My Computer.
3. If you want to change the default size (50 MB) of the vault, type the desired value in the **Vault size** field.
4. Type the desired password to the vault in the **Password** and **Confirm** fields. Anyone trying to open the vault and access its files must provide the password.
5. Click **Create** if you only want to create the vault at the selected location. To create and display the vault as a virtual disk drive in My Computer, click **Create&Open**.

Acronis Internet Security will immediately inform you about the result of the operation. If an error has occurred, use the error message to troubleshoot the error. Click **OK** to close the window.

Note

It may be convenient to save all file vaults to the same location. In this way, you can find them quicker.

19.1.2. Open Vault

In order to access and work with the files stored in a vault, you must open the vault. When you open the vault, a virtual disk drive appears in My Computer. The drive is labeled with the drive letter assigned to the vault.

To open a vault, follow these steps:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Encryption > File Encryption** and do one of the following:
   - Select the vault from the table, click **Choose Action** above the file vaults table and select **Open File Vault** from the menu.
   - Right-click the vault in the table and select **Open**.

Note

If a previously created vault does not appear in the table, click **Choose Action**, select **Add an existing vault** and browse to its location.

A new window will appear.

3. The vault name and path on the disk are displayed. Choose a drive letter from the menu.
4. Type the vault password in the **Password** field.
5. Click **Open**.

Acronis Internet Security will immediately inform you about the result of the operation. If an error has occurred, use the error message to troubleshoot the error.

19.1.3. Lock Vault

When you are done with your work in a file vault, you must lock it in order to protect your data. By locking the vault, the corresponding virtual disk drive disappears from My Computer. Consequently, access to the data stored in the vault is completely blocked.

To lock a vault, open Acronis Internet Security and, depending on the user interface view mode, proceed as follows:

Intermediate View

Go to **File Storage** and do one of the following:

- Click the file vault in the **File Encryption** area and select **Lock** from the menu.
- Click **Lock File Vault** in the Quick Tasks area.

  A wizard will appear to help you lock a vault. You can navigate through the wizard using the **Next** and **Back** buttons. To exit the wizard, click **Cancel**.

  1. **Select File Vault**

     Here you can specify the vault to lock.

  2. **Confirm**

     This is where you can review chosen operations.

  3. **Finish**

     This is where you can view operation result.

Expert View

Go to **Encryption > File Encryption** and do one of the following:

- Select the vault from the table, click **Choose Action** above the file vaults table and select **Lock File Vault** from the menu.

- Right-click the vault in the table and select **Lock**.

Acronis Internet Security will immediately inform you about the result of the operation. If an error has occurred, use the error message to troubleshoot the error. Click **OK** to close the window.

19.1.4. Change Vault Password

The vault must be locked before you can change its password. To change the password of a vault, follow these steps:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Encryption > File Encryption** and do one of the following.
   - Select the vault from the table, click **Choose Action** above the file vaults table and select **Change Password** from the menu.
   - Right-click the vault in the table and select **Change password**.

   A new window will appear.
3. Type the current password of the vault in the **Old password** field.
4. Type the new password of the vault in the **New password** and **Confirm new password** fields.

   Note

   The password must have at least 8 characters. For a strong password, use a combination of uppercase and lowercase letters, numbers and special characters (such as #, $ or @).

5. Click **OK** to change the password.

Acronis Internet Security will immediately inform you about the result of the operation. If an error has occurred, use the error message to troubleshoot the error. Click **OK** to close the window.

19.1.5. Add Files to Vault

To add files to a vault, open Acronis Internet Security and, depending on the user interface view mode, proceed as follows:

Intermediate View

Go to **File Storage** and click **Add File to Vault** in the Quick Tasks area.

A wizard will appear to help you add files to a vault. You can navigate through the wizard using the **Next** and **Back** buttons. To exit the wizard, click **Cancel**.

1. **Select files & folders**

Click **Add target** to select the files/folders that will be added to the vault.

2. **Select File Vault**

   You can select an existing vault, browse for a previously created vault or create a new one in which to add the files.

3. **Create File Vault**

   If you have chosen to create a new vault, this is where you specify the necessary information about it. For more information, please refer to "*Create Vault*" (p. 114)

4. **Enter password**

   If you have selected a locked vault, you must enter the password to open it.

5. **Confirm**

   This is where you can review chosen operations.

6. **File Vault Content**

   This is where you can view the vault content.

Expert View

1. Go to **Encryption > File Encryption**.
2. Select from the vaults table the vault you want to add files in. If the vault is locked, you must first open it (right-click it and select **Open vault**).
3. The File Vault Content table appears. Right-click inside it and select **Add files / folders**.
4. Select the files / folders you want to add to the vault.
5. Click **OK** to copy the selected objects into the vault.

19.1.6. Remove Files from Vault

To remove a file from a vault, open Acronis Internet Security and, depending on the user interface view mode, proceed as follows:

Intermediate View

Go to **File Storage** and click **Remove Vault Files** in the Quick Tasks area.

A wizard will appear to help you remove files from a vault. You can navigate through the wizard using the **Next** and **Back** buttons. To exit the wizard, click **Cancel**.

1. **Select File Vault**

   Here you can specify the vault to remove files from.

2. **Enter password**

If you have selected a locked vault, you must enter the password to open it.

3. **File Vault Content**

   Select the files/folders that will be removed from the vault.

4. **Confirm**

   This is where you can review chosen operations.

5. **Finish**

   This is where you can view the operation result.

Expert View

1. Go to **Encryption > File Encryption**.
2. Select from the vaults table the vault containing the file to be removed. If the vault is locked, you must first open it (right-click it and select **Open vault**).
3. Right-click the file to be removed from the table that displays the vault content and select **Delete**.

19.1.7. View Vault Contents

To view the contents of a file vault, open Acronis Internet Security and, depending on the user interface view mode, proceed as follows:

Intermediate View

Go to **File Storage** and do one of the following:

- Click **View File Vault** in the Quick Tasks area.
- Click the file vault in the **File Encryption** area and select **View** in the menu that appears.

A wizard will appear to help you view the files in the vault. You can navigate through the wizard using the **Next** and **Back** buttons. To exit the wizard, click **Cancel**.

1. **Select File Vault**

   Here you can specify the vault to view files from.

2. **Enter password**

   If you have selected a locked vault, you must enter the password to open it.

3. **Confirm**

   This is where you can review chosen operations.

4. **File Vault Content**

   This is where you can view the operation result.

Expert View

1. Go to **Encryption > File Encryption**.
2. Select from the vaults table the vault whose contents you want to see. If the vault is locked, you must first open it (right-click it and select **Open vault**).

   The table at the bottom displays the content of the selected vault.

19.1.8. Delete File Vault

To delete a file vault, open Acronis Internet Security and, depending on the user interface view mode, proceed as follows:

Intermediate View

1. Go to **File Storage**.
2. Click the file vault in the **File Encryption** area.
3. If the vault is open, select **Lock** in the menu that appears and then click the vault again. If the vault is locked, move to the next step.
4. Select **Delete** in the menu that appears.

Expert View

1. Go to **Encryption > File Encryption**.
2. Select the vault from the table, click **Choose Action** above the file vaults table and select **Delete Vault** from the menu.
3. Confirm the action by clicking **Yes** in the window that appears.

Important
When you delete a file vault all its contents are also deleted.

19.2. Managing File Vaults From Windows

Acronis Internet Security integrates into Windows to help you manage your file vaults more easily.

The Windows contextual menu appears whenever you right-click a file or folder on your computer or objects on your desktop. Simply point to Acronis Internet Security File Vault in this menu and you gain access to all available vault operations.

Additionally, whenever you open (mount) a vault a new logical partition (a new drive) will appear. Just open My Computer and you will see a new drive based on your file vault. You will be able to do file operations on it (copy, delete, change, etc). The files are protected as long as they reside on this drive (because a password is required for the mounting operation). When finished, lock (unmount) your vault in order to start protecting its content.

You can easily identify the Acronis Internet Security file vaults on your computer by the Acronis Internet Security icon and the `.bvd` extension.

19.2.1. Create Vault

Keep in mind that a vault is actually just a file with the `.bvd` extension. Only when you open the vault, a virtual disk drive appears in My Computer and you can safely store files inside it. When creating a vault, you must specify where and under which name to save it on your computer. You must also specify a password to protect its content. Only users who know the password can open the vault and access the documents and data stored inside it.

To create a vault, follow these steps:

1. Right-click on your Desktop or in a folder on your computer, point to **Acronis Internet Security File Vault** and select **Create File Vault**. A new window will appear.
2. Specify the location and the name of the vault file.
   - Click **Browse**, select the location of the vault and save the vault file under the desired name.
   - Type the name and the path of the vault file on the disk in the corresponding fields.
3. Choose a drive letter from the menu. When you open the vault, a virtual disk drive labeled with the selected letter appears in My Computer.
4. Type the desired password to the vault in the **Password** and **Confirm** fields. Anyone trying to open the vault and access its files must provide the password.
5. Select **Format drive** to format the virtual drive assigned to the vault. You must format the drive before you can add files to the vault.
6. If you want to change the default size (50 MB) of the vault, type the desired value in the **Vault size** field.
7. Click **Create** if you only want to create the vault at the selected location. To create and display the vault as a virtual disk drive in My Computer, click **Create&Open**.

Acronis Internet Security will immediately inform you about the result of the operation. If an error has occurred, use the error message to troubleshoot the error. Click **OK** to close the window.

Note
It may be convenient to save all file vaults to the same location. In this way, you can find them quicker.

19.2.2. Open Vault

In order to access and work with the files stored in a vault, you must open the vault. When you open the vault, a virtual disk drive appears in My Computer. The drive is labeled with the drive letter assigned to the vault.

To open a vault, follow these steps:

1. Locate on your computer the `.bvd` file representing the vault you want to open.
2. Right-click the file, point to **Acronis Internet Security File Vault** and select **Open**. Quicker alternatives would be to double-click the file, or to right-click it and select **Open**. A new window will appear.
3. Choose a drive letter from the menu.
4. Type the vault password in the **Password** field.
5. Click **Open**.

Acronis Internet Security will immediately inform you about the result of the operation. If an error has occurred, use the error message to troubleshoot the error. Click **OK** to close the window.

19.2.3. Lock Vault

When you are done with your work in a file vault, you must lock it in order to protect your data. By locking the vault, the corresponding virtual disk drive disappears from My Computer. Consequently, access to the data stored in the vault is completely blocked.

To lock a vault, follow these steps:

1. Open My Computer (click the start Windows Start menu and then **My Computer**).
2. Identify the virtual disk drive corresponding to the vault you want to close. Look for the drive letter you assigned to the vault when you opened it.
3. Right-click the respective virtual disk drive, point to **Acronis Internet Security File Vault** and click **Close**.

You can also right-click the `.bvd` file representing the vault, point to **Acronis Internet Security File Vault** and click **Close**.

Acronis Internet Security will immediately inform you about the result of the operation. If an error has occurred, use the error message to troubleshoot the error. Click **OK** to close the window.

Note

If several vaults are open, you may want to use the Acronis Internet Security Expert View interface. If you go to **Encryption**, File Encryption tab, you can see a table

which provides information on the existing vaults. This information includes whether the vault is open and, if so, the drive letter it was assigned.

19.2.4. Add to File Vault

Before you can add files or folders to a vault, you must open the vault. Once a vault is open, you can easily store files or folders inside it using the contextual menu. Right-click the file or folder you want to copy to a vault, point to **Acronis Internet Security File Vault** and click **Add to File Vault**.

- If only one vault is open, the file or folder is copied directly to that vault.
- If several vaults are open, you will be prompted to choose the vault to copy the item to. Select from the menu the drive letter corresponding to the desired vault and click **OK** to copy the item.

You can also use the virtual disk drive corresponding to the vault. Follow these steps:

1. Open My Computer (click the start Windows Start menu and then **My Computer**).
2. Enter the virtual disk drive corresponding to the vault. Look for the drive letter you assigned to the vault when you opened it.
3. Copy-paste or drag&drop files and folders directly to this virtual disk drive.

19.2.5. Remove from File Vault

In order to remove files or folders from a vault, the vault must be open. To remove files or folders from a vault, follow these steps:

1. Open My Computer (click the start Windows Start menu and then **My Computer**).
2. Enter the virtual disk drive corresponding to the vault. Look for the drive letter you assigned to the vault when you opened it.
3. Remove files or folders as you normally do in Windows (for example, right-click a file you want to delete and select **Delete**).

19.2.6. Change Vault Password

The password protects the content of a vault from unauthorized access. Only users who know the password can open the vault and access the documents and data stored inside it.

The vault must be locked before you can change its password. To change the password of a vault, follow these steps:

1. Locate on your computer the `.bvd` file representing the vault.
2. Right-click the file, point to **Acronis Internet Security File Vault** and select **Change Vault Password**. A new window will appear.

3. Type the current password of the vault in the **Old Password** field.
4. Type the new password of the vault in the **New Password** and **Confirm New Password** fields.

Note

The password must have at least 8 characters. For a strong password, use a combination of uppercase and lowercase letters, numbers and special characters (such as #, $ or @).

5. Click **OK** to change the password.

Acronis Internet Security will immediately inform you about the result of the operation. If an error has occurred, use the error message to troubleshoot the error. Click **OK** to close the window.

20. Game / Laptop Mode

The Game / Laptop Mode module allows you to configure the special operation modes of Acronis Internet Security:

- Game Mode temporarily modifies the product settings so as to minimize the resource consumption when you play.
- Laptop Mode prevents scheduled tasks from running when the laptop is running on battery in order to save battery power.
- Silent Mode temporarily modifies the product settings so as to minimize the interruptions when you watch movies or presentations.

20.1. Game Mode

Game Mode temporarily modifies protection settings so as to minimize their impact on system performance. While in Game Mode, the following settings are applied:

- All Acronis Internet Security alerts and pop-ups are disabled.
- The Acronis Internet Security real-time protection level is set to **Permissive**.
- The Acronis Internet Security firewall is set to **Allow all**. This means that all new connections (both incoming and outgoing) are automatically allowed, regardless of the port and protocol being used.
- Updates are not performed by default.

Note
To change this setting, go to Update>Settings and clear the **Don't update if Game Mode is on** check box.

By default, Acronis Internet Security automatically enters Game Mode when you start a game from the Acronis Internet Security's list of known games or when an application goes to full screen. You can manually enter Game Mode using the default `Ctrl+Alt+Shift+G` hotkey. It is strongly recommended that you exit Game Mode when you finished playing (you can use the same default `Ctrl+Alt+Shift+G` hotkey).

Note
While in Game Mode, you can see the letter G over the Acronis Internet Security icon.

To configure Game Mode:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.

2. Go to **Game/Laptop Mode > Game Mode**.

At the top of the section, you can see the status of the Game Mode. You can click **Game Mode is enabled** or **Game Mode is turned off** to change the current status.

20.1.1. Configuring Automatic Game Mode

Automatic Game Mode allows Acronis Internet Security to automatically enter Game Mode when a game is detected. You can configure the following options:

- **Use the default list of games provided by Acronis Internet Security** - to automatically enter Game Mode when you start a game from the Acronis Internet Security's list of known games. To view this list, click **Manage Games** and then **Games List**.
- **Full screen action** - you can choose to automatically enter Game Mode or Silent Mode when an application goes to full screen.
- **Ask me if I want to add applications in full screen to the whitelist** - to be prompted to add a new game to the whitelist when you leave full screen. By adding a new game to the whitelist, the next time you start it Acronis Internet Security will automatically enter Game Mode.

Note

If you do not want Acronis Internet Security to automatically enter Game Mode, clear the **Automatic Game Mode is enabled** check box.

20.1.2. Managing the Game List

Acronis Internet Security automatically enters Game Mode when you start an application from the game list. To view and manage the game list, click **Manage Games**. A new window will appear.

New applications are automatically added to the list when:

- You start a game from the Acronis Internet Security's list of known games. To view this list, click **Games List**.
- After leaving full screen, you add the application to the game list from the prompt window.

If you want to disable Automatic Game Mode for a specific application from the list, clear its corresponding check box. You should disable Automatic Game Mode for regular applications that go to full screen, such as web browsers and movie players.

To manage the game list, you can use the buttons placed at the top of the table:

- **Add** - add a new application to the game list.
- **Remove** - remove an application from the game list.

- **Edit** - edit an existing entry in the game list.

20.1.3. Adding or Editing Games

When you add or edit an entry from the game list, a new window will appear.

Click **Browse** to select the application or type the full path to the application in the edit field.

If you do not want to automatically enter Game Mode when the selected application is started, select **Disable**.

Click **OK** to add the entry to the game list.

20.1.4. Configuring Game Mode Settings

To configure the behaviour on scheduled tasks, use these options:

- **Enable this module to modify Antivirus scan tasks schedules** - to prevent scheduled scan tasks from running while in Game Mode. You can choose one of the following options:

Option	Description
Skip Task	Do not run the scheduled task at all.
Postpone Task	Run the scheduled task immediately after you exit Game Mode.

To automatically disable the Acronis Internet Security firewall while in Game Mode, follow these steps:

1. Click **Advanced Settings**. A new window will appear.
2. Select the **Set Firewall on Allow All** check box.
3. Click **OK** to save the changes.

20.1.5. Changing Game Mode Hotkey

You can manually enter Game Mode using the default `Ctrl+Alt+Shift+G` hotkey. If you want to change the hotkey, follow these steps:

1. Click **Advanced Settings**. A new window will appear.
2. Under the **Enable Game Mode Hotkeys** option, set the desired hotkey:
   - Choose the modifier keys you want to use by checking one the following: Control key (`Ctrl`), Shift key (`Shift`) or Alternate key (`Alt`).
   - In the edit field, type the letter corresponding to the regular key you want to use.

For example, if you want to use the `Ctrl+Alt+D` hotkey, you must check only `Ctrl` and `Alt` and type `D`.

Note
To disable the hotkey, clear the **Enable Game Mode Hotkeys** check box.

3. Click **OK** to save the changes.

20.2. Laptop Mode

Laptop Mode is especially designed for laptop and notebook users. Its purpose is to minimize Acronis Internet Security's impact on power consumption while these devices are running on battery.

While in Laptop Mode, scheduled tasks are by default not performed.

Acronis Internet Security detects when your laptop has switched to battery power and it automatically enters Laptop Mode. Likewise, Acronis Internet Security automatically exits Laptop Mode, when it detects the laptop is no longer running on battery.

To configure Laptop Mode:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Game/Laptop Mode > Laptop Mode**.

You can see whether Laptop Mode is enabled or not. If Laptop Mode is enabled, Acronis Internet Security will apply the configured settings while the laptop is running on battery.

20.2.1. Configuring Laptop Mode Settings

To configure the behaviour on scheduled tasks, use these options:

- **Enable this module to modify Antivirus scan tasks schedules** - to prevent scheduled scan tasks from running while in Laptop Mode. You can choose one of the following options:

Option	Description
Skip Task	Do not run the scheduled task at all.
Postpone Task	Run the scheduled task immediately after you exit Laptop Mode.

20.3. Silent Mode

Silent Mode temporarily modifies protection settings so as to minimize their impact on system performance. While in Silent Mode the following settings are applied:

- All Acronis Internet Security alerts and pop-ups are disabled.
- The Acronis Internet Security firewall is set to **Allow all**. This means that all new connections (both incoming and outgoing) are automatically allowed, regardless of the port and protocol being used.
- Scheduled scan tasks are by default disabled.

By default, Acronis Internet Security automatically enters Silent Mode when you watch a movie or a presentation or when an application goes to full screen. It is strongly recommended that you exit Silent Mode when you finished watching the movie or the presentation.

Note
While in Silent Mode, you can see a slight modification of the little Acronis Internet Security icon located next to your computer clock.

To configure Silent Mode:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Game/Laptop Mode > Silent Mode**.

At the top of the section, you can see the status of the Silent Mode. You can click **Silent Mode is enabled** or **Silent Mode is disabled** to change the current status.

20.3.1. Configuring Full Screen Action

You can configure the following options:

- **Full screen action** - you can choose to automatically enter Game Mode or Silent Mode when an application goes to full screen.
- **Ask me if I want to add applications in full screen to the whitelist** - to be prompted to add a new application to the whitelist when you leave full screen. By adding a new application to the whitelist, the next time you start it Acronis Internet Security will automatically enter Silent Mode.

Note
If you do not want Acronis Internet Security to automatically enter Silent Mode, clear the **Full Screen Action** check box.

20.3.2. Configuring Silent Mode Settings

To configure the behaviour on scheduled tasks, use these options:

- **Enable this module to modify Antivirus scan tasks schedules** - to prevent scheduled scan tasks from running while in Silent Mode. You can choose one of the following options:

Option	Description
Skip Task	Do not run the scheduled task at all.
Postpone Task	Run the scheduled task immediately after you exit Silent Mode.

21. Home Network

The Network module allows you to manage the Acronis Internet Security products installed on your home computers from a single computer. To access the Home Network module, open Acronis Internet Security and, depending on the user interface view mode, proceed as follows:

Intermediate View
Go to the **Network** tab.

Expert View
Go to **Home Network**.

Note
You can also add a shortcut to My Tools.

To be able to manage the Acronis Internet Security products installed on your home computers, you must follow these steps:

1. Enable the Acronis Internet Security home network on your computer. Set your computer as Server.
2. Go to each computer you want to manage and join the network (set the password). Set each computer as Regular.
3. Go back to your computer and add the computers you want to manage.

21.1. Enabling the Acronis Internet Security Network

To enable the Acronis Internet Security home network, follow these steps:

1. Click **Enable Network**. You will be prompted to configure the home management password.
2. Type the same password in each of the edit fields.
3. Set the role of the computer in the Acronis Internet Security home network:
   - **Server Computer** - select this option on the computer that will be used to manage all the other ones.
   - **Regular Computer** - select this option on the computers that will be managed by the Server Computer.
4. Click **OK**.

You can see the computer name appearing in the network map.

The **Disable Network** button appears.

21.2. Adding Computers to the Acronis Internet Security Network

Any computer will be automatically added to the network if it meets the following criteria:

- the Acronis Internet Security home network was enabled on it.
- the role was set to Regular Computer.
- the password set when enabling the network is the same as the password set on the Server Computer.

Note

In Expert View, you can scan the home network for computers meeting the criteria at any time by clicking the **Auto discover** button.

To manually add a computer to the Acronis Internet Security home network from the Server Computer, follow these steps:

1. Click **Add Computer**.
2. Type the home management password and click **OK**. A new window will appear.

   You can see the list of computers in the network. The icon meaning is as follows:

    Indicates an online computer with no Acronis Internet Security products installed.

    Indicates an online computer with Acronis Internet Security installed.

    Indicates an offline computer with Acronis Internet Security installed.
3. Do one of the following:
   - Select from the list the name of the computer to add.
   - Type the IP address or the name of the computer to add in the corresponding field.
4. Click **Add**. You will be prompted to enter the home management password of the respective computer.
5. Type the home management password configured on the respective computer.
6. Click **OK**. If you have provided the correct password, the selected computer name will appear in the network map.

21.3. Managing the Acronis Internet Security Network

Once you have successfully created a Acronis Internet Security home network, you can manage all Acronis Internet Security products from a single computer.

If you move the mouse cursor over a computer from the network map, you can see brief information about it (name, IP address, number of issues affecting the system security, Acronis Internet Security registration status).

If you click a computer name in the network map, you can see all the administrative tasks you can run on the remote computer.

- **Set a settings password on a remote PC**

  Allows you to create a password to restrict access to Acronis Internet Security settings on this PC.

- **Run an on-demand scan task**

  Allows you to run an on-demand scan on the remote computer. You can perform any of the following scan tasks: My Documents Scan, System Scan or Deep System Scan.

- **Fix all issues on this PC**

  Allows you to fix the issues that are affecting the security of this computer by following the Fix All Issues wizard.

- **View History/Events**

  Allows you access to the **History&Events** module of the Acronis Internet Security product installed on this computer.

- **Update Now**

  Intitiates the Update process for the Acronis Internet Security product installed on this computer.

- **Set Parental Control Profile**

  Allows you to set the age category to be used by the Parental Control web filter on this computer.

- **Set as Update Server for this network**

  Allows you to set this computer as update server for all Acronis Internet Security products installed on the computers in this network. Using this option will reduce internet traffic, because only one computer in the network will connect to the internet to download updates.

- **Remove PC from home network**

  Allows you to remove a PC from the network.

When the Acronis Internet Security interface is in Intermediate View, you can run several tasks on all managed computers at the same time by clicking the corresponding buttons.

- **Scan All** - allows you to scan all managed computers at the same time.
- **Update All** allows you to update all managed computers at the same time.

Before running a task on a specific computer, you will be prompted to provide the local home management password. Type the home management password and click **OK**.

Note

If you plan to run several tasks, you might want to select **Don't show this message again this session**. By selecting this option, you will not be prompted again for this password during the current session.

22. Update

New malware is found and identified every day. This is why it is very important to keep Acronis Internet Security up to date with the latest malware signatures.

If you are connected to the Internet through broadband or DSL, Acronis Internet Security takes care of this itself. By default, it checks for updates when you turn on your computer and every **hour** after that.

If an update is detected, you may be asked to confirm the update or the update is performed automatically, depending on the automatic update settings.

The update process is performed on the fly, meaning that the files to be updated are replaced progressively. In this way, the update process will not affect product operation and, at the same time, any vulnerability will be excluded.

Important
To be protected against the latest threats keep the **Automatic Update** enabled.

Updates come in the following ways:

- **Updates for the antivirus engines** - as new threats appear, the files containing virus signatures must be updated to ensure permanent up-to-date protection against them. This update type is also known as **Virus Definitions Update**.
- **Updates for the antispam engines** - new rules will be added to the heuristic and URL filters and new images will be added to the Image filter. This will help increase the effectiveness of your Antispam engine. This update type is also known as **Antispam Update**.
- **Updates for the antispyware engines** - new spyware signatures will be added to the database. This update type is also known as **Antispyware Update**.
- **Product upgrades** - when a new product version is released, new features and scan techniques are introduced to the effect of improving the product's performance. This update type is also known as **Product Update**.

22.1. Performing an Update

The automatic update can be done anytime you want by clicking **Update Now**. This update is also known as **Update by user request**.

To update Acronis Internet Security, depending on the user interface mode, proceed as follows:

Basic View

Click the **Update Now** icon in the Protect your PC area.

Intermediate View

Go to the **Security** tab and click **Update Now** in the Quick Tasks area on the left side of the window.

Expert View

Go to **Update > Update**.

The **Update** module will connect to the Acronis Internet Security update server and will verify if any update is available. If an update was detected, depending on the options set in the Manual Update Settings section, you will be asked to confirm the update or the update will be made automatically.

Important

It may be necessary to restart the computer when you have completed the update. We recommend doing it as soon as possible.

Note

If you are connected to the Internet through a dial-up connection, then it is recommended to regularly update Acronis Internet Security by user request. For more information, please refer to *"How to Update Acronis Internet Security on a Slow Internet Connection"* (p. 155).

22.2. Configuring Update Settings

The updates can be performed from the local network, over the Internet, directly or through a proxy server. By default, Acronis Internet Security will check for updates every hour, over the Internet, and install the available updates without alerting you.

To configure the update settings:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Update > Settings**.
3. Configure the settings as needed. To find out what an option does, keep the mouse over it and read the description displayed at the bottom of the window.
4. Click **Apply** to save the changes.

To apply the default settings, click **Default**.

22.2.1. Setting Update Locations

To set the update locations, use the options from the **Update Location Settings** category.

Note

Configure these settings only if you are connected to a local network that stores Acronis Internet Security malware signatures locally or if you connect to the Internet through a proxy server.

To modify one of the update locations, enter the address of the local update server in the corresponding field.

Note

We recommend you to set as primary update location the local mirror and to leave the alternate update location unchanged, as a fail-safe plan in case the local mirror becomes unavailable.

If your computer connects to the Internet through a proxy server, select **Use proxy** and then configure the proxy settings. For more information, please refer to "Connection Settings" (p. 35)

22.2.2. Configuring Automatic Update

To configure the update process performed automatically by Acronis Internet Security, use the options in the **Automatic Update Settings** category.

You can specify the number of hours between two consecutive checks for updates in the **Update every** field. By default, the update time interval is set to 1 hour.

To specify how the automatic update process should be performed, select one of the following options:

- **Silent update** - Acronis Internet Security automatically downloads and implements the update.
- **Prompt before downloading updates** - every time an update is available, you will be prompted before downloading it.
- **Prompt before installing updates** - every time an update was downloaded, you will be prompted before installing it.

22.2.3. Configuring Manual Update

To specify how the manual update (update by user request) should be performed, select one of the following options in the **Manual Update Settings** category:

- **Silent update** - the manual update will be performed automatically in the background, without user intervention.
- **Prompt before downloading updates** - every time an update is available, you will be prompted before downloading it.

22.2.4. Configuring Advanced Settings

To prevent the Acronis Internet Security update process from interfering with your work, configure the options in the **Advanced Settings** category:

- **Wait for reboot, instead of prompting** - If an update requires a reboot, the product will keep working with the old files until the system is rebooting. The user will not be prompted for rebooting, therefore the Acronis Internet Security update process will not interfere with the user's work.
- **Enable update sharing (P2P)** - If you want to minimize the impact of the network traffic on system performance during updates, use the update sharing option. Acronis Internet Security uses ports 8880 - 8889 for peer-to-peer update.
- **Upload Acronis Internet Security files from this PC** - Acronis Internet Security lets you share the latest antivirus signatures available on your PC with other Acronis Internet Security users.
- **Do not update if a scan is in progress** - Acronis Internet Security will not update if a scan process is running. This way, the Acronis Internet Security update process will not interfere with the scan tasks.

Note

If Acronis Internet Security is updated while a scan is in progress, the scan process will be aborted.

- **Do not update if Game Mode is on** - Acronis Internet Security will not update if the Game Mode is turned on. In this way, you can minimize the product's influence on system performance during games.

How To

23. How Do I Scan Files and Folders?

Scanning is easy and flexible with Acronis Internet Security. There are several ways to set Acronis Internet Security to scan files and folders for viruses and other malware:

- Using Windows Contextual Menu
- Using Scan Tasks
- Using Scan Activity Bar

Once you initiate a scan, the Antivirus Scan wizard will appear and guide you through the process. For detailed information about this wizard, please refer to "*Antivirus Scan Wizard*" (p. 46).

23.1. Using Windows Contextual Menu

This is the easiest and recommended way to scan a file or folder on your computer. Right-click the object you want to scan and select **Scan with Acronis Internet Security** from the menu. Follow the Antivirus Scan wizard to complete the scan.

Typical situations when you would use this scanning method include the following:

- You suspect a specific file or folder to be infected.
- Whenever you download from the Internet files that you think they might be dangerous.
- Scan a network share before copying files to your computer.

23.2. Using Scan Tasks

If you want to scan your computer or specific folders regularly, you should consider using scan tasks. Scan tasks instruct Acronis Internet Security what locations to scan, and which scanning options and actions to apply. Moreover, you can schedule them to run on a regular basis or at a specific time.

To scan your computer using scan tasks, you must open the Acronis Internet Security interface and run the desired scan task. Depending on the user interface view mode, different steps are to be followed to run the scan task.

Running Scan Tasks in Basic View

In Basic View, you can run a number of pre-configured scan tasks. Click the **Security** button and choose the desired scan task. Follow the Antivirus Scan wizard to complete the scan.

Running Scan Tasks in Intermediate View

In Intermediate View, you can run a number of pre-configured scan tasks. You can also configure and run custom scan tasks to scan specific locations on your computer using custom scanning options. Follow these steps to run a scan task in Intermediate View:

1. Click the **Security** tab.
2. On the left-side Quick Tasks area, click **Full System Scan** and choose the desired scan task. To configure and run a custom scan, click **Custom Scan**.
3. Follow the Antivirus Scan wizard to complete the scan. If you chose to run a custom scan, you must first complete the Custom Scan wizard.

Running Scan Tasks in Expert View

In Expert View, you can run all of the pre-configured scan tasks, and also change their scanning options. Moreover, you can create customized scan tasks if you want to scan specific locations on your computer. Follow these steps to run a scan task in Expert View:

1. Click **Antivirus** on the left-side menu.
2. Click the **Virus Scan** tab. Here you can find a number of default scan tasks and you can create your own scan tasks.
3. Double-click the scan task you want to run.
4. Follow the Antivirus Scan wizard to complete the scan.

23.3. Using Scan Activity Bar

The **Scan activity bar** is a graphic visualization of the scanning activity on your system. This small window is by default available only in Expert View.

You can use the Scan activity bar to quickly scan files and folders. Drag & drop the file or folder you want to be scanned onto the Scan activity bar. Follow the Antivirus Scan wizard to complete the scan.

Scan Activity Bar

Note
For more information, please refer to "*Scan Activity Bar*" (p. 3).

24. How Do I Create a Custom Scan Task?

To create a scan task, open Acronis Internet Security and depending on the user interface view mode, proceed as follows:

Intermediate View

Go to the **Security** tab and click **Custom Scan** in the Quick Tasks area on the left side of the window.

A wizard will appear to help you create a scan task. You can navigate through the wizard using the **Next** and **Back** buttons. To exit the wizard, click **Cancel**.

1. **Welcome**
2. **Choose Target**

   Click **Add Target** to select the files or folders to be scanned.

   Click **Advanced Settings**. In the **Overview** tab, adjust the scanning options by moving the cursor on the slider. If you want to configure the scanning options in detail, click **Custom**. Go to the **Scheduler** tab to select when the task will run.
3. **Finish**

   This is where you can enter the task name and optionally add the scan to the Quick Tasks area.

   Click **Start Scan** to create the task and launch the scan wizard.

Expert View

1. Go to **Antivirus > Virus Scan**.
2. Click **New Task**. A new window will appear.

   Note

   You can also right-click a pre-defined scan task, such as **Deep System Scan** and choose **Clone Task**. This is useful when creating new tasks, as you can modify the settings of the task you have duplicated.
3. In the **Overview** tab, enter the task name and adjust the scanning options by moving the cursor on the slider.

   If you want to configure the scanning options in detail, click **Custom**.
4. Go to the **Paths** tab to select the scan target. Click **Add Item(s)** to select the files or folders to be scanned.
5. Go to the **Scheduler** tab to select when the task will run.
6. Click **Ok** to save the task. The new task will appear under the User defined tasks and can be edited, removed or run at any moment from this window.

25. How Do I Schedule a Computer Scan?

Scanning your computer periodically is a best practice to keep your computer free from malware. Acronis Internet Security allows you to schedule scan tasks so that you can automatically scan your computer.

To schedule Acronis Internet Security to scan your computer, follow these steps:

1. Open Acronis Internet Security.
2. Depending on the user interface view mode, proceed as follows:

   Intermediate View
   Go to the **Security** tab, click **Full System Scan** in the Quick Tasks area and select **Schedule My Scans**.

   Expert View
   Click **Antivirus** on the left-side menu.
3. Click the **Virus Scan** tab. Here you can find a number of default scan tasks and you can create your own scan tasks.

   - System tasks are available and can run on every Windows user account.
   - User tasks are only available to and can only be run by the user who created them.

   These are the default scan tasks that you can schedule:

   Full System Scan
   Scans the entire system, except for archives. In the default configuration, it scans for all types of malware other than rootkits.

   Quick Scan
   Quick Scan uses in-the-cloud scanning to detect malware running in your system. Running a Quick Scan usually takes less than a minute and uses a fraction of the system resources needed by a regular virus scan.

   Auto-logon Scan
   Scans the items that are run when a user logs on to Windows. To use this task, you must schedule it to run at system startup. By default, the autologon scan is disabled.

   Deep System Scan
   Scans the entire system. In the default configuration, it scans for all types of malware threatening your system's security, such as viruses, spyware, adware, rootkits and others.

   My Documents
   Use this task to scan important current user folders: `My Documents`, `Desktop` and `StartUp`. This will ensure the safety of your documents, a safe workspace and clean applications running at startup.

If none of these scan tasks suit your needs, you can create a new scan task, which you can then schedule to run as needed.

4. Choose a scan task and select **Schedule**. A new window will appear.
5. Schedule the task to run as needed:
   - To run the scan task one-time only, select **Once** and specify the start date and time.
   - To run the scan task after the system startup, select **On system startup**. You can specify how long after the startup the task should start running (in minutes).
   - To run the scan task on a regular basis, select **Periodically** and specify the frequency and the start date and time.

   Note

   For example, to scan your computer every Saturday at 2 AM, you must configure the schedule as follows:

   a. Select **Periodically**.

   b. In the **At every** field, type 1 and then select **weeks** from the menu. In this way, the task is run once every week.

   c. Set as start date the first Saturday to come.

   d. Set as start time `2:00:00 AM`.

6. Click **OK** to save the schedule. The scan task will run automatically according to the schedule you have defined. If the computer is shut down when the schedule is due, the task will run the next time you start your computer.

26. How Do I Use File Vaults?

The Acronis Internet Security File Vault enables you to create encrypted, password-protected logical drives (or vaults) on your computer where you can securely store your confidential and sensitive documents. Physically, the vault is a file stored on the local hard drive having the .bvd extension.

When you create a file vault, two aspects are important: the size and the password. The default 50 MB size should be enough for your private documents, Excel files and others the like. However, for videos or other large files you may need more space.

To securely store your confidential or sensitive files or folders in Acronis Internet Security file vaults, follow these steps:

- **Create a file vault and set a strong password for it.**

  To create a vault, right-click an empty area of the Desktop or in a folder on your computer, point to Acronis Internet Security File Vault and select **Create vault**.

  A new window will appear. Proceed as follows:

  1. Click **Browse**, select the location of the vault and save the vault file under the desired name.
  2. Choose a drive letter from the menu. When you open the vault, a virtual disk drive labeled with the selected letter appears in **My Computer**.
  3. Type the vault password in the **Password** and **Confirm** fields.
  4. If you want to change the default size (50 MB) of the vault, type the desired value in the **Vault size** field.
  5. Click Create if you only want to create the vault at the selected location. To create and display the vault as a virtual disk drive in **My Computer** click **Create and Open**.

  Note

  When you open the vault, a virtual disk drive appears in **My Computer**. The drive is labeled with the drive letter assigned to the vault.

- **Add the files or folders you want to keep safe to the vault.**

  In order to add a file to a vault, you must first open the vault.

  1. Browse to the .bvd vault file.
  2. Right-click the vault file, point to Acronis Internet Security File Vault and select **Open**.
  3. In the window that appears, select a drive letter to assign to the vault, enter the password and click **Open**.

You can now perform operations on the drive that corresponds to the desired file vault using Windows Explorer, just as you would with a regular drive. To add a file to an open vault, you can also right-click the file, point to Acronis Internet Security File Vault and select **Add to file vault**.

- **Keep the vault locked at all times.**

  Only open vaults when you need to access them or manage their content. To lock a vault, right-click the corresponding virtual disk drive from **My Computer**, point to **Acronis Internet Security File Vault** and select **Lock**.

- **Make sure not to delete the .bvd vault file.**

  Deleting the file also deletes the vault contents.

For more information about operating with file vaults, please refer to *"File Encryption"* (p. 114).

27. How Do I Create Windows User Accounts?

A Windows user account is a unique profile that includes all the settings, privileges and personal files for each user.

Windows accounts let the home PC administrator control access for each user.

Setting up user accounts comes in handy when the PC is used by both parents and children – a parent can set up accounts for each child.

Choose which operating system you have to find out how to create Windows accounts.

- Windows XP:
  1. Log on to your computer as an administrator.
  2. Click Start, click Control Panel, and then click User Accounts.
  3. Click Create a new account.
  4. Type the name for the user. You can use the person's full name, first name, or a nickname. Then click Next.
  5. For the account type, choose Limited, and then Create Account. Limited accounts are appropriate for children because they cannot make system-wide changes or install certain applications.
  6. Your new account will have been created and you will see it listed in the Manage Accounts screen.
- Windows Vista or Windows 7:
  1. Log on to your computer as an administrator.
  2. Click Start, click Control Panel, and then click User Accounts.
  3. Click Create a new account.
  4. Type the name for the user. You can use the person's full name, first name, or a nickname. Then click Next.
  5. For the account type, click Standard, and then Create Account. Limited accounts are appropriate for children because they cannot make system-wide changes or install certain applications.
  6. Your new account will have been created and you will see it listed in the Manage Accounts screen.

Note

Now that you have added new user accounts, you can create passwords for the accounts.

28. How Do I Update Acronis Internet Security Using a Proxy Server?

Normally, Acronis Internet Security automatically detects and imports the proxy settings from your system. If you connect to the Internet through a proxy server, you may need to find the proxy settings and configure Acronis Internet Security accordingly. To find out how to do this, please refer to "*How Do I Find Out My Proxy Settings?*" (p. 173).

After finding the proxy settings, follow these steps:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **General > Settings**.
3. Click **Proxy Settings** from **Connection Settings**.
4. Enter the proxy settings in the corresponding fields.
5. Click **OK**.

Note

If this information was not helpful, you can contact Acronis Internet Security for support as described in section "*Support*" (p. 171).

Troubleshooting and Getting Help

29. Troubleshooting

This chapter presents some problems you may encounter when using Acronis Internet Security and provides you with possible solutions to these problems. Most of these problems can be solved through the appropriate configuration of the product settings.

If you cannot find your problem here, or if the presented solutions do not solve it, you can contact the Acronis technical support representatives as presented in chapter "*Support*" (p. 171).

29.1. Scan Doesn't Start

This type of issue can have two main causes:

- **A previous Acronis Internet Security installation which was not completely removed or a faulty Acronis Internet Security installation**.

  If this is the case, the easiest solution to follow is to remove Acronis Internet Security completely from the system and then reinstall it.

- **Acronis Internet Security is not the only security solution installed on your system**.

  In this case, follow these steps:

  1. Remove the other security solution.
  2. Remove Acronis Internet Security completely from the system.
  3. Reinstall Acronis Internet Security on the system.

If this information was not helpful, you can contact Acronis Internet Security for support as described in section "*Support*" (p. 171).

29.2. I Can no Longer Use an Application

This issue occurs when you are trying to use a program which was working normally before installing Acronis Internet Security.

You may encounter one of these situations:

- You could receive a message from Acronis Internet Security that the program is trying to make a modification to the system.
- You could receive an error message from the program you're trying to use.

This type of situation occurs when the Active Virus Control module mistakenly detects some applications as malicious.

Active Virus Control is a Acronis Internet Security module which constantly monitors the applications running on your system and reports those with potentially malicious

behavior. Since this feature is based on a heuristic system, there may be cases when legitimate applications are reported by Active Virus Control.

When this situation occurs, you can exclude the respective application from being monitored by Active Virus Control.

To add the program to the exclusions list, follow these steps:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus > Shield**.
3. Click **Advanced Settings**.
4. In the new window go to the **Exclusions** tab, click the **Add** button and browse to the location of the program's .exe file (usually located in the `C:\Program Files`).
5. Click **OK** to save the changes and close the window.
6. Close the Acronis Internet Security window and check if the issue still occurs.

If this information was not helpful, you can contact Acronis Internet Security for support as described in section "*Support*" (p. 171).

29.3. I Cannot Connect to the Internet

You may notice that a program can no longer connect to the Internet or access network services after installing Acronis Internet Security.

The Troubleshoot wizard will help you identify and solve the connection issue. To start the wizard, open Acronis Internet Security and, depending on the user interface mode, proceed as follows:

Intermediate View
: Go to the **Security** tab and click **Configure Firewall** in the Quick Tasks area on the left side of the window. Select the **Settings** tab in the new window that appears and click **Troubleshoot**.

Expert View
: Go to **Firewall > Settings** and click **Troubleshoot**.

Follow the three-step guided procedure to start the troubleshooting. You can navigate through the wizard using the **Next** button. To exit the wizard, click **Cancel**.

1. **Welcome**

   Select **I am trying to access the Internet and the action fails**.

2. **Identify Problem**

   Click **Choose Application** and **Browse** to locate the program's .exe file (usually located in the `C:\Program Files`, i.e. Firefox.exe). Click **Add**.

3. **Recommended Solution**

   Choose **Yes, allow access**. Click **Finish** and check if the issue still occurs.

If this information was not helpful, you can contact Acronis Internet Security for support as described in section "*Support*" (p. 171).

29.4. I Cannot Use a Printer

Depending on the network you are connected to, the Acronis Internet Security firewall may block the connection between your computer and a network printer.

In this case, the best solution is to configure Acronis Internet Security to automatically allow connections to and from the respective printer.

The Troubleshoot wizard will help you identify and solve the connection issue. To start the wizard, open Acronis Internet Security and, depending on the user interface mode, proceed as follows:

Intermediate View
: Go to the **Security** tab and click **Configure Firewall** in the Quick Tasks area on the left side of the window. Select the **Settings** tab in the new window that appears and click **Troubleshoot**.

Expert View
: Go to **Firewall > Settings** and click **Troubleshoot**.

Follow the three-step guided procedure to start the troubleshooting. You can navigate through the wizard using the **Next** button. To exit the wizard, click **Cancel**.

1. **Welcome**

   Select **I am trying to print and the action fails**.

2. **Identify Problem**

   Click **Choose Printer**. Select the printer from the list, either by name or by IP address. If you cannot find the device in the list, enter the IP address manually in the edit field. Click **Add**.

3. **Recommended Solution**

   Choose **Yes, allow access**. Click **Finish** and check if the issue still occurs.

If the Troubleshoot wizard indicates that the problem is not caused by the Acronis Internet Security firewall on your computer, check for other potential causes, such as the following:

- The firewall on the other computer may block file and printer sharing with your computer.

  ▶ If the Windows Firewall is used, it can be configured to allow file and printer sharing as follows: open the Windows Firewall settings window, **Exceptions** tab and select the **File and Printer Sharing** check box.

- If another firewall program is used, please refer to its documentation or help file.

- General conditions that may prevent using or connecting to the shared printer:
  - You may need to log on to a Windows administrator account to access the shared printer.
  - Permissions are set for the shared printer to allow access to specific computer and users only. If you are sharing your printer, check the permissions set for the printer to see if the user on the other computer is allowed access to the printer. If you are trying to connect to a shared printer, check with the user on the other computer if you have permission to connect to the printer.
  - The printer connected to your computer or to the other computer is not shared.
  - The shared printer is not added on the computer.

  Note
  To learn how to manage printer sharing (share a printer, set or remove permissions for a printer, connect to a network printer or to a shared printer), go to the Windows Help and Support Center (in the Start menu, click **Help and Support**).

- Access to a network printer may be restricted to specific computers or users only. You should check with the network administrator if you have permission to connect to that printer.

If this information was not helpful, you can contact Acronis Internet Security for support as described in section "*Support*" (p. 171).

29.5. I Cannot Share Files with Another Computer

Depending on the network you are connected to, the Acronis Internet Security firewall may block the connection between your system and another computer. As a result, you may no longer share files with the other computer. In this case, the best solution is to configure Acronis Internet Security to automatically allow connections to and from the respective system.

The Troubleshoot wizard will help you identify and solve the connection issue. To start the wizard, open Acronis Internet Security and, depending on the user interface mode, proceed as follows:

Intermediate View
: Go to the **Security** tab and click **Configure Firewall** in the Quick Tasks area on the left side of the window. Select the **Settings** tab in the new window that appears and click **Troubleshoot**.

Expert View
: Go to **Firewall > Settings** and click **Troubleshoot**.

Follow the three-step guided procedure to start the troubleshooting. You can navigate through the wizard using the **Next** button. To exit the wizard, click **Cancel**.

1. **Welcome**

   Select **I am trying to access a computer in my network and the action fails**.

2. **Identify Problem**

   Click **Choose Computer**. Select the computer from the list, either by name or by IP address. If you cannot find the computer in the list, enter the IP address manually in the edit field. Click **Add**.

3. **Recommended Solution**

   Choose **Yes, allow access**. Click **Finish** and check if the issue still occurs.

If this information was not helpful, you can contact Acronis Internet Security for support as described in section "*Support*" (p. 171).

29.6. My Internet Is Slow

This situation may appear after you install Acronis Internet Security. The issue could be caused by errors in the Acronis Internet Security firewall configuration.

To troubleshoot this situation, follow these steps:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Firewall > Settings**.
3. Clear the **Firewall is enabled** check box to temporarily disable the firewall.
4. Check if you can connect to the Internet with the Acronis Internet Security firewall disabled.
   - If you still cannot connect to the Internet, the issue may not be caused by Acronis Internet Security. You should contact your Internet Service Provider to verify if the connection is operational on their side.

     If you receive confirmation from your Internet Service Provider that the connection is operational on their side and the issue still persists, contact Acronis Internet Security as described in section "*Support*" (p. 171).
   - If you manage to connect to the Internet after disabling the Acronis Internet Security firewall, follow these steps:
     a. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
     b. Go to **Firewall > Settings** and select the box in order to enable the Firewall.

c. Click **Advanced Settings**, select **Enable Internet Connection Sharing** and clear **Block Port Scans**.

d. Go to the **Network** tab in the main window.

e. Pull down the drop-down menu from the **Network Type** column and select **Home/ Office**.

f. Go to the **Generic** column and set it to **Yes**. Set the **Stealth Mode** to **Remote**.

g. Check if you can connect to the Internet.

If this information was not helpful, you can contact Acronis Internet Security for support as described in section "*Support*" (p. 171).

29.7. How to Update Acronis Internet Security on a Slow Internet Connection

If you have a slow Internet connection (such as dial-up), errors may occur during the update process.

To keep your system up to date with the latest Acronis Internet Security malware signatures, follow these steps:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Update > Settings**.
3. Under **Manual Update Settings**, select **Prompt before downloading updates**.
4. Click **Apply** and go to the **Update** tab.
5. Click **Update Now** and you will see that a new window will appear.
6. Select only **Signatures updates** and then click **Ok**.
7. Acronis Internet Security will download and install only the malware signature updates.

29.8. Acronis Internet Security Services Are Not Responding

This article helps you troubleshoot the *Acronis Internet Security Services are not responding* error. You may encounter this error as follows:

- The Acronis Internet Security icon in the system tray is grayed out and a pop-up informs you that the Acronis Internet Security services are not responding.
- The Acronis Internet Security window indicates that the Acronis Internet Security services are not responding.

The error may be caused by one of the following conditions:

- an important update is being installed.
- temporary communication errors between the Acronis Internet Security services.
- some of the Acronis Internet Security services are stopped.
- other security solutions running on your computer at the same time with Acronis Internet Security.
- viruses on your system affect the normal operation of Acronis Internet Security.

To troubleshoot this error, try these solutions:

1. Wait a few moments and see if anything changes. The error may be temporary.
2. Restart the computer and wait a few moments until Acronis Internet Security is loaded. Open Acronis Internet Security to see if the error persists. Restarting the computer usually solves the problem.
3. Check if you have any other security solution installed as they may disrupt the normal operation of Acronis Internet Security. If this is the case, we recommend you to remove all of the other security solutions and then reinstall Acronis Internet Security.
4. If the error persists, there may be a more serious problem (for example, you may be infected with a virus that interferes with Acronis Internet Security). Please contact Acronis Internet Security for support as described in section "*Support*" (p. 171).

29.9. Antispam Filter Does Not Work Properly

This article helps you troubleshoot the following problems concerning the Acronis Internet Security Antispam filtering operation:

- A number of legitimate e-mail messages are marked as [spam].
- Many spam messages are not marked accordingly by the antispam filter.
- The antispam filter does not detect any spam message.

29.9.1. Legitimate Messages Are Marked as [spam]

Legitimate messages are marked as [spam] simply because they look like spam to the Acronis Internet Security antispam filter. You can normally solve this problem by adequately configuring the Antispam filter.

Acronis Internet Security automatically adds the receivers of your e-mail messages to a Friends List. The e-mail messages received from the contacts in the Friends list are considered to be legitimate. They are not verified by the antispam filter and, thus, they are never marked as [spam].

The automatic configuration of the Friends list does not prevent the detection errors that may occur in these situations:

- You receive a lot of solicited commercial mail as a result of subscribing on various websites. In this case, the solution is to add the e-mail addresses from which you receive such e-mail messages to the Friends list.
- A significant part of your legitimate mail is from people to whom you never e-mailed before, such as customers, potential business partners and others. Other solutions are required in this case.

If you are using one of the mail clients Acronis Internet Security integrates into, try the following solutions:

1. Indicate detection errors. This is used to train the Learning Engine (Bayesian) of the antispam filter and it helps prevent future detection errors. The Learning Engine analyzes the indicated messages and learns their patterns. The next e-mail messages that fit the same patterns will not be marked as `[spam]`.
2. Decrease antispam protection level. By decreasing the protection level, the antispam filter will need more spam indications to classify an e-mail message as spam. Try this solution only if many legitimate messages (including solicited commercial messages) are incorrectly detected as spam.
3. Retrain the Learning Engine (Bayesian filter). Try this solution only if the previous solutions did not offer satisfactory results.

Note

Acronis Internet Security integrates into the most commonly used mail clients through an easy-to-use antispam toolbar. For a complete list of supported mail clients, please refer to "*Supported E-mail Clients and Protocols*" (p. 67).

If you are using a different mail client, you cannot indicate detection errors and train the Learning Engine. To solve the problem, try decreasing the antispam protection level.

Add Contacts to Friends List

If you are using a supported mail client, you can easily add the senders of legitimate messages to the Friends list. Follow these steps:

1. In your mail client, select an e-mail message from the sender that you want to add to the Friends list.
2. Click the **Add Friend** button on the Acronis Internet Security antispam toolbar.
3. You may be asked to acknowledge the addresses added to the Friends list. Select **Don't show this message again** and click **OK**.

You will always receive e-mail messages from this address no matter what they contain.

If you are using a different mail client, you can add contacts to the Friends list from the Acronis Internet Security interface. Follow these steps:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Click **Antispam** on the left-side menu.
3. Click the **Status** tab.
4. Click **Manage Friends**. A configuration window will appear.
5. Type the e-mail address you always want to receive e-mail messages from and click the button to add the address to the Friends List.
6. Click **OK** to save the changes and close the window.

Indicate Detection Errors

If you are using a supported mail client, you can easily correct the antispam filter (by indicating which e-mail messages should not have been marked as [spam]). Doing so will considerably improve the efficiency of the antispam filter. Follow these steps:

1. Open your mail client.
2. Go to the junk mail folder where spam messages are moved.
3. Select the legitimate message incorrectly marked as [spam] by Acronis Internet Security.
4. Click the **Add Friend** button on the Acronis Internet Security antispam toolbar to add the sender to the Friends list. You may need to click **OK** to acknowledge. You will always receive e-mail messages from this address no matter what they contain.
5. Click the **Not Spam** button on the Acronis Internet Security antispam toolbar (normally located in the upper part of the mail client window). This indicates to the Learning Engine that the selected message is not spam. The e-mail message will be moved to the Inbox folder. The next e-mail messages that fit the same patterns will no longer be marked as [spam].

Decrease Antispam Protection Level

To decrease the antispam protection level, follow these steps:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Click **Antispam** on the left-side menu.
3. Click the **Status** tab.
4. Move the slider lower on the scale.

It is recommended to decrease protection by just one level and then wait enough time to evaluate the results. If many legitimate e-mail messages are still being

marked as [spam], you can further decrease the protection level. If you notice that many spam messages are not detected, you should not decrease the protection level.

Retrain Learning Engine (Bayesian)

Before training the Learning Engine (Bayesian), prepare a folder containing only SPAM messages and another one containing only legitimate messages. The Learning Engine will analyze them and learn the characteristics that define the spam or legitimate messages that you usually receive. In order for the training to be efficient, there must be over 50 messages in each category.

To reset the Bayesian database and retrain the Learning Engine, follow these steps:

1. Open your mail client.
2. On the Acronis Internet Security antispam toolbar, click the **Wizard** button to start the antispam configuration wizard.
3. Click **Next**.
4. Select **Skip this step** and click **Next**.
5. Select **Clear antispam filter database** and click **Next**.
6. Select the folder containing legitimate messages and click **Next**.
7. Select the folder containing SPAM messages and click **Next**.
8. Click **Finish** to start the training process.
9. When training is completed, click **Close**.

Ask for Help

If this information was not helpful, you can contact Acronis Internet Security for support as described in section "*Support*" (p. 171).

29.9.2. Many Spam Messages Are Not Detected

If you are receiving many spam messages that are not marked as [spam], you must configure the Acronis Internet Security antispam filter so as to improve its efficiency.

If you are using one of the mail clients Acronis Internet Security integrates into, try the following solutions one at a time:

1. Indicate undetected spam messages. This is used to train the Learning Engine (Bayesian) of the antispam filter and it usually improves antispam detection. The Learning Engine analyzes the indicated messages and learns their patterns. The next e-mail messages that fit the same patterns will be marked as [spam].

2. Add spammers to the Spammers list. The e-mail messages received from addresses in the Spammers list are automatically marked as [spam].
3. Increase antispam protection level. By increasing the protection level, the antispam filter will need less spam indications to classify an e-mail message as spam.
4. Retrain the Learning Engine (Bayesian filter). Use this solution when antispam detection is very unsatisfactory and indicating undetected spam messages no longer works.

Note

Acronis Internet Security integrates into the most commonly used mail clients through an easy-to-use antispam toolbar. For a complete list of supported mail clients, please refer to "*Supported E-mail Clients and Protocols*" (p. 67).

If you are using a different mail client, you cannot indicate spam messages and train the Learning Engine. To solve the problem, try increasing the antispam protection level and adding spammers to the Spammers list.

Indicate Undetected Spam Messages

If you are using a supported mail client, you can easily indicate which e-mail messages should have been detected as spam. Doing so will considerably improve the efficiency of the antispam filter. Follow these steps:

1. Open your mail client.
2. Go to the Inbox folder.
3. Select the undetected spam messages.
4. Click the **Is Spam** button on the Acronis Internet Security antispam toolbar (normally located in the upper part of the mail client window). This indicates to the Learning Engine that the selected messages are spam. They are immediately marked as [spam] and moved to the junk mail folder. The next e-mail messages that fit the same patterns will be marked as [spam].

Add Spammers to Spammers List

If you are using a supported mail client, you can easily add the senders of the spam messages to the Spammers list. Follow these steps:

1. Open your mail client.
2. Go to the junk mail folder where spam messages are moved.
3. Select the messages marked as [spam] by Acronis Internet Security.
4. Click the **Add Spammer** button on the Acronis Internet Security antispam toolbar.

5. You may be asked to acknowledge the addresses added to the Spammers list. Select **Don't show this message again** and click **OK**.

If you are using a different mail client, you can manually add spammers to the Spammers list from the Acronis Internet Security interface. It is convenient to do this only when you have received several spam messages from the same e-mail address. Follow these steps:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Click **Antispam** on the left-side menu.
3. Click the **Status** tab.
4. Click **Manage Spammers**. A configuration window will appear.
5. Type the spammer's e-mail address and click the button to add the address to the Spammers List.
6. Click **OK** to save the changes and close the window.

Increase Antispam Protection Level

To increase the antispam protection level, follow these steps:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Click **Antispam** on the left-side menu.
3. Click the **Status** tab.
4. Move the slider higher on the scale.

Retrain Learning Engine (Bayesian)

Before training the Learning Engine (Bayesian), prepare a folder containing only SPAM messages and another one containing only legitimate messages. The Learning Engine will analyze them and learn the characteristics that define the spam or legitimate messages that you usually receive. In order for the training to be efficient, there must be over 50 messages in each folder.

To reset the Bayesian database and retrain the Learning Engine, follow these steps:

1. Open your mail client.
2. On the Acronis Internet Security antispam toolbar, click the **Wizard** button to start the antispam configuration wizard.
3. Click **Next**.
4. Select **Skip this step** and click **Next**.
5. Select **Clear antispam filter database** and click **Next**.

6. Select the folder containing legitimate messages and click **Next**.
7. Select the folder containing SPAM messages and click **Next**.
8. Click **Finish** to start the training process.
9. When training is completed, click **Close**.

Ask for Help

If this information was not helpful, you can contact Acronis Internet Security for support as described in section "*Support*" (p. 171).

29.9.3. Antispam Filter Does Not Detect Any Spam Message

If no spam message is marked as `[spam]`, there may be a problem with the Acronis Internet Security Antispam filter. Before troubleshooting this problem, make sure it is not caused by one of the following conditions:

- The Acronis Internet Security Antispam protection is available only for e-mail clients configured to receive e-mail messages via the POP3 protocol. This means the following:
  - ▶ E-mail messages received via web-based e-mail services (such as Yahoo, Gmail, Hotmail or other) are not filtered for spam by Acronis Internet Security.
  - ▶ If your e-mail client is configured to receive e-mail messages using other protocol than POP3 (for example, IMAP4), the Acronis Internet Security Antispam filter does not check them for spam.

  Note

  POP3 is one of the most widely used protocols for downloading e-mail messages from a mail server. If you do not know the protocol that your e-mail client uses to download e-mail messages, ask the person who configured your e-mail client.

- Acronis Internet Security 2011 doesn't scan Lotus Notes POP3 traffic.

You should also verify the following possible causes:

1. Make sure Antispam is enabled.
   a. Open Acronis Internet Security.
   b. Click the **Options** button in the upper-right corner of the window and choose **Preferences**.
   c. In the Security Settings category, check the antispam status.

   If Antispam is disabled, this is what is causing your problem. Enable Antispam and monitor the antispam operation to see if the problem is fixed.
2. Although very unlikely, you may want to check if you (or someone else) configured Acronis Internet Security not to mark spam messages as `[spam]`.

a. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
b. Click **Antispam** on the left-side menu and then the **Settings** tab.
c. Make sure option **Mark spam messages in subject** is selected.

A possible solution is to repair or reinstall the product. However, you may want to contact Acronis for support instead, as described in section "*Support*" (p. 171).

30. Removing Malware from Your System

Malware can affect your system in many different ways and the Acronis Internet Security approach depends on the type of malware attack. Because viruses change their behavior frequently, it is difficult to establish a pattern for their behavior and their actions.

There are situations when Acronis Internet Security cannot automatically remove the malware infection from your system. In such cases, your intervention is required.

If you cannot find your problem here, or if the presented solutions do not solve it, you can contact the Acronis technical support representatives as presented in chapter "*Support*" (p. 171).

30.1. What to Do When Acronis Internet Security Finds Viruses on Your Computer?

You may find out there is a virus on your computer in one of these ways:

- You scanned your computer and Acronis Internet Security found infected items on it.
- A virus alert informs you that Acronis Internet Security blocked one or multiple viruses on your computer.

In such situations, update Acronis Internet Security to make sure you have the latest malware signatures and run a Deep System Scan to analyze the system.

As soon as the deep scan is over, select the desired action for the infected items (Disinfect, Delete, Move to quarantine).

If the selected action could not be taken and the scan log reveals an infection which could not be deleted, you have to remove the file(s) manually:

The first method can be used in Normal mode:

1. Turn off the Acronis Internet Security real-time antivirus protection. To find out how to do this, please refer to "*How Do I Enable / Disable the Real Time Protection?*" (p. 174).
2. Display hidden objects in Windows. To find out how to do this, please refer to "*How Do I Display Hidden Objects in Windows?*" (p. 175).
3. Browse to the location of the infected file (check the scan log) and delete it.
4. Turn on the Acronis Internet Security real-time antivirus protection.

In case the first method failed to remove the infection, follow these steps:

1. Reboot your system and enter in Safe Mode. To find out how to do this, please refer to "*How Do I Restart in Safe Mode?*" (p. 172).

2. Display hidden objects in Windows.
3. Browse to the location of the infected file (check the scan log) and delete it.
4. Reboot your system and enter in normal mode.

If this information was not helpful, you can contact Acronis Internet Security for support as described in section "*Support*" (p. 171).

30.2. If Your System Does Not Start

If your system does not start, use Acronis Rescue CD.

Acronis Rescue CD is a bootable CD capable to scan and disinfect all existing hard drives before your operating system starts. It can also help you save data from your compromised Windows PC to a removable device.

Important

To obtain an ISO image of Acronis Rescue CD, contact us as presented in "*Support*" (p. 171). You can then burn the .iso file to a CD or DVD using a tool of your choice.

Scanning the System with the Acronis Rescue CD

To scan your system with the Acronis Rescue CD, follow these steps:

1. Set up the BIOS of your computer to boot off the CD.
2. Put the CD in the drive and reboot the computer.
3. Wait until the Acronis Rescue CD screen appears. Select the option to start Acronis Rescue CD and then press **Enter**.
4. Wait for the boot process to complete. This may take a while.
5. As soon as the boot process has completed, the Acronis Internet Security signatures are updated automatically and a scan of all detected hard disk partitions is started.

Saving Data with the Acronis Rescue CD

Let's assume that you cannot start your Windows PC due to some unknown issues. At the same time, you desperately need to access some important data from your computer. This is where Acronis Rescue CD comes in handy.

To save your data from the computer to a removable device, such as an USB flash drive, follow these steps:

1. Set up the BIOS of your computer to boot off the CD.
2. Put the CD in the drive and reboot the computer.
3. Wait until the Acronis Rescue CD screen appears. Select the option to start Acronis Rescue CD and then press **Enter**.

4. Wait for the boot process to complete. This may take a while.
5. As soon as the boot process has completed, the Acronis Internet Security signatures are updated automatically and a scan of all detected hard disk partitions is started. You should wait for the scan to finish.
6. Your hard disk partitions will appear on the desktop. To view the contents of a disk in a window similar to Windows Explorer, double-click it.

Note
When working with the Acronis Rescue CD, you will deal with Linux-type partition names. Disks that were not labeled under Windows will appear as `[LocalDisk-0]` probably corresponding to the `(C:)` Windows-type partition, `[LocalDisk-1]` corresponding to `(D:)` and so on.

7. Plug the removable device into an USB port on your computer. In a few moments a window will appear showing the contents of the device.
8. You can copy files and folders as you would normally do in the Windows environment.

If this information was not helpful, you can contact Acronis Internet Security for support as described in section "*Support*" (p. 171).

30.3. How Do I Clean a Virus in an Archive?

An archive is a file or a collection of files compressed under a special format to reduce the space on disk necessary for storing the files.

Some of these formats are open formats, thus providing Acronis Internet Security the option to scan inside them and then take appropriate actions to remove them.

Other archive formats are partially or fully closed, and Acronis Internet Security can only detect the presence of viruses inside them, but is not able to take any other actions.

If Acronis Internet Security notifies you that a virus has been detected inside an archive and no action is available, it means that removing the virus is not possible due to restrictions on the archive's permission settings.

Here is how you can clean a virus stored in an archive:

1. Identify the archive that includes the virus by performing a Deep System Scan of the system.
2. Turn off the Acronis Internet Security real-time antivirus protection.
3. Go to the location of the archive and decompress it using an archiving application, like WinZip.
4. Identify the infected file and delete it.

5. Delete the original archive in order to make sure the infection is totally removed.
6. Recompress the files in a new archive using an archiving application, like WinZip.
7. Turn on the Acronis Internet Security real-time antivirus protection and run a Deep system scan in order to make sure there is no other infection on the system.

Note

It's important to note that a virus stored in an archive is not an immediate threat to your system, since the virus has to be decompressed and executed in order to infect your system.

If this information was not helpful, you can contact Acronis Internet Security for support as described in section "*Support*" (p. 171).

30.4. How Do I Clean a Virus in an E-Mail Archive?

Acronis Internet Security can also identify viruses in e-mail databases and e-mail archives stored on disk.

Sometimes it is necessary to identify the infected message using the information provided in the scan report, and delete it manually.

Here is how you can clean a virus stored in an e-mail archive:

1. Scan the e-mail database with Acronis Internet Security.
2. Turn off the Acronis Internet Security real-time antivirus protection.
3. Open the scan report and use the identification information (Subject, From, To) of the infected messages to locate them in the e-mail client.
4. Delete the infected messages. Most e-mail clients also move the deleted message to a recovery folder, from which it can be recovered. You should make sure the message is deleted also from this recovery folder.
5. Compact the folder storing the infected message.
   - In Outlook Express: On the File menu, click Folder, then Compact All Folders.
   - In Microsoft Outlook: On the File menu, click Data File Management. Select the personal folders (.pst) files you intend to compact, and click Settings. Click Compact.
6. Turn on the Acronis Internet Security real-time antivirus protection.

If this information was not helpful, you can contact Acronis Internet Security for support as described in section "*Support*" (p. 171).

30.5. What to Do When Acronis Internet Security Detected a Clean File as Infected?

There are cases when Acronis Internet Security mistakenly flags a legitimate file as being a threat (a false positive). To correct this error, add the file to the Acronis Internet Security Exclusions area:

1. Turn off the Acronis Internet Security real-time antivirus protection. To find out how to do this, please refer to "*How Do I Enable / Disable the Real Time Protection?*" (p. 174).
2. Display hidden objects in Windows. To find out how to do this, please refer to "*How Do I Display Hidden Objects in Windows?*" (p. 175).
3. Restore the file from the Quarantine area.
4. Insert the file in the Exclusions area.
5. Turn on the Acronis Internet Security real-time antivirus protection.

If this information was not helpful, you can contact Acronis Internet Security for support as described in section "*Support*" (p. 171).

30.6. How to Clean the Infected Files from System Volume Information

The System Volume Information folder is a zone on your hard drive created by the Operating System and used by Windows for storing critical information related to the system configuration.

The Acronis Internet Security engines can detect any infected files stored by the System Volume Information, but being a protected area it may not be able to remove them.

The infected files detected in the System Restore folders will appear in the scan log as follows:

```
?:\System Volume Information\_restore{B36120B2-BA0A-4E5D-…
```

To completely and immediately remove the infected file or files in the data store, disable and re-enable the System Restore feature.

When System Restore is turned off, all the restore points are removed.

When System Restore is turned on again, new restore points are created as the schedule and events require.

In order to disable the System Restore follow these steps:

- **For Windows XP:**

1. Follow this path: **Start** → **All Programs** → **Accessories** → **System Tool** → **System Restore**
2. Click **System Restore Settings** located on the left hand side of the window.
3. Select the **Turn off System Restore** check box on all drives, and click **Apply**.
4. When you are warned that all existing Restore Points will be deleted, click **Yes** to continue.
5. To turn on the System Restore, clear the **Turn off System Restore** check box on all drives, and click **Apply**.

- **For Windows Vista:**
  1. Follow this path: **Start** → **Control Panel** → **System and Maintenance** → **System**
  2. In the left pane, click **System Protection**.

     If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
  3. To turn off the System Restore clear the check boxes corresponding to each drive and click **Ok**.
  4. To turn on the System Restore select the check boxes corresponding to each drive and click **Ok**.
- **For Windows 7:**
  1. Click **Start**, right-click **Computer** and click **Properties**.
  2. Click **System protection** link in the left pane.
  3. In the **System protection** options, select each drive letter and click **Configure**.
  4. Select **Turn off system protection** and click **Apply**.
  5. Click **Delete**, click **Continue** when prompted and then click **Ok**.

If this information was not helpful, you can contact Acronis Internet Security for support as described in section "*Support*" (p. 171).

30.7. What Are the Password-Protected Files in the Scan Log?

This is only a notification which indicates that Acronis Internet Security has detected these files are either protected with a password or by some form of encryption.

Most commonly, the password-protected items are:

- Files that belong to another security solution.
- Files that belong to the operating system.

In order to actually scan the contents, these files would need to either be extracted or otherwise decrypted.

Should those contents be extracted, Acronis Internet Security's real-time scanner would automatically scan them to keep your computer protected. If you want to scan those files with Acronis Internet Security, you have to contact the product manufacturer in order to provide you with more details on those files.

Our recommendation to you is to ignore those files because they are not a threat for your system.

30.8. What Are the Skipped Items in the Scan Log?

All files that appear as Skipped in the scan report are clean.

For increased performance, Acronis Internet Security does not scan files that have not changed since the last scan.

30.9. What Are the Over-Compressed Files in the Scan Log?

The over-compressed items are elements which could not be extracted by the scanning engine or elements for which the decryption time would have taken too long making the system unstable.

Overcompressed means that Acronis Internet Security skipped scanning within that archive because unpacking it proved to take up too many system resources. The content will be scanned on real time access if needed.

30.10. Why Did Acronis Internet Security Automatically Delete an Infected File?

If an infected file is detected, Acronis Internet Security will automatically attempt to disinfect it. If disinfection fails, the file is moved to quarantine in order to contain the infection.

For particular types of malware, disinfection is not possible because the detected file is entirely malicious. In such cases, the infected file is deleted from the disk.

This is usually the case with installation files that are downloaded from untrustworthy websites. If you find yourself in such a situation, download the installation file from the manufacturer's website or other trusted website.

31. Support

If you need help or additional information on Acronis Internet Security 2011, use the contact information provided below.

Acronis Inc.
23 3rd Avenue
Burlington, MA 01803
USA

Buy: http://www.acronis.com/buy/abs2011

Web: http://www.acronis.com/homecomputing/products/backup-security/

In order to contact support (Webmail, Phone, Chat), please use the wizard set at: http://www.acronis.com/support/ > Contact Support > Start here.

Availability: 24x7

Media: E-mail (Webmail), Phone, Chat.

32. Useful Information

This chapter presents some important procedures that you must be aware before starting to troubleshoot a technical issue.

Troubleshooting a technical situation in Acronis Internet Security requires a few Windows insights, therefore the next steps are mostly related to the Windows operating system.

32.1. How Do I Remove Other Security Solutions?

The main reason for using a security solution is to provide protection and safety for your data. But what happens when you have more than one security product on the same system?

When you use more than one security solution on the same computer, the system becomes unstable. The Acronis Internet Security 2011 installer automatically detects other security programs and offers you the option to uninstall them.

If you did not remove the other security solutions during the initial installation, follow these steps:

- For **Windows XP**:
  1. Click **Start**, go to **Control Panel** and double-click **Add / Remove programs**.
  2. Wait a few moments until the list of installed software is displayed.
  3. Find the name of the program you want to remove and select **Remove**.
  4. Wait for the uninstall process to complete, then reboot your system.
- For **Windows Vista** and **Windows 7**:
  1. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.
  2. Wait a few moments until the installed software list is displayed.
  3. Find the name of the program you want to remove and select **Uninstall**.
  4. Wait for the uninstall process to complete, then reboot your system.

If you fail to remove the other security solution from your system, get the uninstall tool from the vendor website or contact them directly in order to provide you with the uninstall guidelines.

32.2. How Do I Restart in Safe Mode?

Safe mode is a diagnostic operating mode, used mainly to troubleshoot problems affecting normal operation of Windows. Such problems range from conflicting drivers to viruses preventing Windows from starting normally. In Safe Mode only a few applications work and Windows loads just the basic drivers and a minimum of

operating system components. This is why most viruses are inactive when using Windows in Safe Mode and they can be easily removed.

To start Windows in Safe Mode:

1. Restart the computer.
2. Press the **F8** key several times before Windows starts in order to access the boot menu.
3. Select **Safe Mode** in the boot menu and press **Enter**.
4. Wait while Windows loads in Safe Mode.
5. This process ends with a confirmation message. Click **Ok** to acknowledge.
6. To start Windows normally, simply reboot the system.

32.3. Am I Using a 32 bit or a 64 bit Version of Windows?

To find out if you have a 32 bit or a 64 bit operating system, follow these steps:

- For **Windows XP**:
  1. Click **Start**.
  2. Locate **My Computer** on the **Start** menu.
  3. Right-click **My Computer** and select **Properties**.
  4. If you see **x64 Edition** listed under **System**, you are running the 64 bit version of Windows XP.

     If you don't see **x64 Edition** listed, you are running a 32 bit version of Windows XP.
- For **Windows Vista** and **Windows 7**:
  1. Click **Start**.
  2. Locate **Computer** on the **Start** menu.
  3. Right-click **Computer** and select **Properties**.
  4. Look under **System** in order to check the information about your system.

32.4. How Do I Find Out My Proxy Settings?

In order to find these settings, follow these steps :

- For Internet Explorer 8:
  1. Open Internet Explorer.
  2. Select **Tools** > **Internet Options**.
  3. In the **Connections** tab click **LAN settings**.

4. Look under **Use a proxy server for your LAN** and you should see the **Address** and **Port** of the proxy.

- For Mozilla Firefox 3.6:
  1. Open Firefox.
  2. Select **Tools** > **Options**.
  3. In the **Advanced** tab go to **Network** tab.
  4. Click **Settings**.
- For Opera 10.51:
  1. Open Opera.
  2. Select **Tools** > **Preferences**.
  3. In the **Advanced** tab go to **Network** tab.
  4. Click **Proxy servers** button to open the proxy settings dialog.

32.5. How Do I Enable / Disable the Real Time Protection?

Acronis Internet Security provides continuous, real-time protection against a wide range of malware threats by scanning all accessed files, e-mail messages and the communications through Instant Messaging Software applications (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

Normally the real-time protection in Acronis Internet Security is enabled and you should not turn it off.

When you are trying to troubleshoot a problem or to remove a virus, you may need to disable the real-time protection. They address one of these situations:

- A slowdown issue with the system after installing Acronis Internet Security
- An issue with one of the programs or applications after installing Acronis Internet Security
- Error messages which could appear shortly after installing Acronis Internet Security

Follow these steps so that you may enable/ disable real-time protection temporarily:

1. Open Acronis Internet Security, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus** > **Shield**.
3. Clear the **Real-time protection is enabled** check box to temporarily disable antivirus protection (or select it if you want to enable the protection).
4. You must confirm your choice by selecting from the menu how long you want the real-time protection to be disabled.

Note

The steps for disabling the real-time protection in Acronis Internet Security should be used as a temporary solution and only for a short period of time.

32.6. How Do I Display Hidden Objects in Windows?

These steps are useful in those cases where you are dealing with a malware situation and you need to find and remove the infected files, which could be hidden.

Follow these steps to display hidden objects in Windows:

1. Click **Start**, go to **Control Panel** and select **Folder Options**.
2. Go to **View** tab.
3. Select **Display contents of system folders** (for Windows XP only).
4. Select **Show hidden files and folders**.
5. Clear **Hide file extensions for known file types**.
6. Clear **Hide protected operating system files**.
7. Click **Apply** and then **Ok**.

Glossary

ActiveX

ActiveX is a model for writing programs so that other programs and the operating system can call them. ActiveX technology is used with Microsoft Internet Explorer to make interactive Web pages that look and behave like computer programs, rather than static pages. With ActiveX, users can ask or answer questions, use push buttons, and interact in other ways with the Web page. ActiveX controls are often written using Visual Basic.

Active X is notable for a complete lack of security controls; computer security experts discourage its use over the Internet.

Adware

Adware is often combined with a host application that is provided at no charge as long as the user agrees to accept the adware. Because adware applications are usually installed after the user has agreed to a licensing agreement that states the purpose of the application, no offense is committed.

However, pop-up advertisements can become an annoyance, and in some cases degrade system performance. Also, the information that some of these applications collect may cause privacy concerns for users who were not fully aware of the terms in the license agreement.

Archive

A disk, tape, or directory that contains files that have been backed up.

A file that contains one or more files in a compressed format.

Backdoor

A hole in the security of a system deliberately left in place by designers or maintainers. The motivation for such holes is not always sinister; some operating systems, for example, come out of the box with privileged accounts intended for use by field service technicians or the vendor's maintenance programmers.

Boot sector

A sector at the beginning of each disk that identifies the disk's architecture (sector size, cluster size, and so on). For startup disks, the boot sector also contains a program that loads the operating system.

Boot virus

A virus that infects the boot sector of a fixed or floppy disk. An attempt to boot from a diskette infected with a boot sector virus will cause the virus to become active in memory. Every time you boot your system from that point on, you will have the virus active in memory.

Browser

Short for Web browser, a software application used to locate and display Web pages. The two most popular browsers are Netscape Navigator and Microsoft Internet Explorer. Both of these are graphical browsers, which means that they can display graphics as well as text. In addition, most modern browsers can present multimedia information, including sound and video, though they require plug-ins for some formats.

Command line

In a command line interface, the user types commands in the space provided directly on the screen using command language.

Cookie

Within the Internet industry, cookies are described as small files containing information about individual computers that can be analyzed and used by advertisers to track your online interests and tastes. In this realm, cookie technology is still being developed and the intention is to target ads directly to what you've said your interests are. It's a double-edge sword for many people because on one hand, it's efficient and pertinent as you only see ads about what you're interested in. On the other hand, it involves actually "tracking" and "following" where you go and what you click. Understandably so, there is a debate over privacy and many people feel offended by the notion that they are viewed as a "SKU number" (you know, the bar code on the back of packages that gets scanned at the grocery check-out line). While this viewpoint may be extreme, in some cases it is accurate.

Disk drive

It's a machine that reads data from and writes data onto a disk.

A hard disk drive reads and writes hard disks.

A floppy drive accesses floppy disks.

Disk drives can be either internal (housed within a computer) or external (housed in a separate box that connects to the computer).

Download

To copy data (usually an entire file) from a main source to a peripheral device. The term is often used to describe the process of copying a file from an online service to one's own computer. Downloading can also refer to copying a file from a network file server to a computer on the network.

E-mail

Electronic mail. A service that sends messages on computers via local or global networks.

Events

An action or occurrence detected by a program. Events can be user actions, such as clicking a mouse button or pressing a key, or system occurrences, such as running out of memory.

False positive

Occurs when a scanner identifies a file as infected when in fact it is not.

Filename extension

The portion of a filename, following the final point, which indicates the kind of data stored in the file.

Many operating systems use filename extensions, e.g. Unix, VMS, and MS-DOS. They are usually from one to three letters (some sad old OSes support no more than three). Examples include "c" for C source code, "ps" for PostScript, "txt" for arbitrary text.

Heuristic

A rule-based method of identifying new viruses. This method of scanning does not rely on specific virus signatures. The advantage of the heuristic scan is that it is not fooled by a new variant of an existing virus. However, it might occasionally report suspicious code in normal programs, generating the so-called "false positive".

IP

Internet Protocol - A routable protocol in the TCP/IP protocol suite that is responsible for IP addressing, routing, and the fragmentation and reassembly of IP packets.

Java applet

A Java program which is designed to run only on a web page. To use an applet on a web page, you would specify the name of the applet and the size (length and width, in pixels) that the applet can utilize. When the web page is accessed, the browser downloads the applet from a server and runs it on the user's machine (the client). Applets differ from applications in that they are governed by a strict security protocol.

For example, even though applets run on the client, they cannot read or write data onto the client's machine. Additionally, applets are further restricted so that they can only read and write data from the same domain that they are served from.

Macro virus

A type of computer virus that is encoded as a macro embedded in a document. Many applications, such as Microsoft Word and Excel, support powerful macro languages.

These applications allow you to embed a macro in a document, and have the macro execute each time the document is opened.

Mail client

An e-mail client is an application that enables you to send and receive e-mail.

Memory

Internal storage areas in the computer. The term memory identifies data storage that comes in the form of chips, and the word storage is used for memory that exists on tapes or disks. Every computer comes with a certain amount of physical memory, usually referred to as main memory or RAM.

Non-heuristic

This method of scanning relies on specific virus signatures. The advantage of the non-heuristic scan is that it is not fooled by what might seem to be a virus, and does not generate false alarms.

Packed programs

A file in a compression format. Many operating systems and applications contain commands that enable you to pack a file so that it takes up less memory. For example, suppose you have a text file containing ten consecutive space characters. Normally, this would require ten bytes of storage.

However, a program that packs files would replace the space characters by a special space-series character followed by the number of spaces being replaced. In this case, the ten spaces would require only two bytes. This is just one packing technique - there are many more.

Path

The exact directions to a file on a computer. These directions are usually described by means of the hierarchical filing system from the top down.

The route between any two points, such as the communications channel between two computers.

Phishing

The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

Polymorphic virus

A virus that changes its form with each file it infects. Since they have no consistent binary pattern, such viruses are hard to identify.

Port

An interface on a computer to which you can connect a device. Personal computers have various types of ports. Internally, there are several ports for connecting disk drives, display screens, and keyboards. Externally, personal computers have ports for connecting modems, printers, mice, and other peripheral devices.

In TCP/IP and UDP networks, an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.

Report file

A file that lists actions that have occurred. Acronis Internet Security maintains a report file listing the path scanned, the folders, the number of archives and files scanned, how many infected and suspicious files were found.

Rootkit

A rootkit is a set of software tools which offer administrator-level access to a system. The term was first used for the UNIX operating systems and it referred to recompiled tools which provided intruders administrative rights, allowing them to conceal their presence so as not to be seen by the system administrators.

The main role of rootkits is to hide processes, files, logins and logs. They may also intercept data from terminals, network connections or peripherals, if they incorporate the appropriate software.

Rootkits are not malicious in nature. For example, systems and even some applications hide critical files using rootkits. However, they are mostly used to hide malware or to conceal the presence of an intruder into the system. When combined with malware, rootkits pose a great threat to the integrity and the security of a system. They can monitor traffic, create backdoors into the system, alter files and logs and avoid detection.

Script

Another term for macro or batch file, a script is a list of commands that can be executed without user interaction.

Spam

Electronic junk mail or junk newsgroup postings. Generally known as any unsolicited e-mail.

Spyware

Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.

Spyware's similarity to a Trojan horse is the fact that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today.

Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's Internet connection. Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability.

Startup items

Any files placed in this folder will open when the computer starts. For example, a startup screen, a sound file to be played when the computer first starts, a reminder calendar, or application programs can be startup items. Normally, an alias of a file is placed in this folder rather than the file itself.

System tray

Introduced with Windows 95, the system tray is located in the Windows taskbar (usually at the bottom next to the clock) and contains miniature icons for easy access to system functions such as fax, printer, modem, volume, and more. Double click or right-click an icon to view and access the details and controls.

TCP/IP

Transmission Control Protocol/Internet Protocol - A set of networking protocols widely used on the Internet that provides communications across interconnected networks of computers with diverse hardware architectures and various operating systems. TCP/IP includes standards for how computers communicate and conventions for connecting networks and routing traffic.

Trojan

A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive.

One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

The term comes from a story in Homer's Iliad, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

Update

A new version of a software or hardware product designed to replace an older version of the same product. In addition, the installation routines for updates often check to make sure that an older version is already installed on your computer; if not, you cannot install the update.

Acronis Internet Security has it's own update module that allows you to manually check for updates, or let it automatically update the product.

Virus

A program or piece of code that is loaded onto your computer without your knowledge and runs against your will. Most viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can copy itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

Virus definition

The binary pattern of a virus, used by the antivirus program to detect and eliminate the virus.

Worm

A program that propagates itself over a network, reproducing itself as it goes. It cannot attach itself to other programs.