



Bitdefender®

Bitdefender Endpoint Security Tools

USER'S GUIDE

Publication date 2015.12.15

Copyright© 2015 Bitdefender

Legal Notice

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from an authorized representative of Bitdefender. The inclusion of brief quotations in reviews may be possible only with the mention of the quoted source. The content can not be modified in any way.

Warning and Disclaimer. This product and its documentation are protected by copyright. The information in this document is provided on an "as is" basis, without warranty. Although every precaution has been taken in the preparation of this document, the authors will not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

This book contains links to third-party Websites that are not under the control of Bitdefender, therefore Bitdefender is not responsible for the content of any linked site. If you access a third-party website listed in this document, you will do so at your own risk. Bitdefender provides these links only as a convenience, and the inclusion of the link does not imply that Bitdefender endorses or accepts any responsibility for the content of the third-party site.

Trademarks. Trademark names may appear in this book. All registered and unregistered trademarks in this document are the sole property of their respective owners, and are respectfully acknowledged.



Table of Contents

Using This Guide	iv
1. Purpose and Intended Audience	iv
2. How to Use This Guide	iv
3. Conventions Used in This Guide	iv
4. Request for Comments	v
1. Getting Started	1
1.1. The System Tray Icon	1
1.2. The Main Window	2
1.2.1. The Notifications Area	3
1.2.2. Events Timeline	4
1.3. The Modules Window	4
1.4. Actions Menu	8
2. Scanning for Malware	10
2.1. Scanning a File or Folder	10
2.2. Running a Quick Scan	10
2.3. Running a Full Scan	11
2.4. Configuring and Running a Custom Scan	11
2.4.1. File Types	12
2.4.2. What to Scan?	13
2.4.3. What to Do?	14
2.5. Checking Scan Logs	15
3. Updates	16
3.1. Types of Updates	16
3.2. Checking If Your Protection Is Up-to-Date	16
3.3. Performing an Update	17
4. Events	18
5. Getting Help	19
Glossary	20

Using This Guide

1. Purpose and Intended Audience

This documentation is intended for the end users of **Bitdefender Endpoint Security Tools**, the Security for Endpoints client software installed on computers and servers to protect them against malware and other Internet threats and to enforce user control policies.

The information presented herein should be easy to understand by anyone who is able to work under Windows.

2. How to Use This Guide

This guide is organized so as to make it easy to find the information you need.

[“Getting Started” \(p. 1\)](#)

Get familiar with the Bitdefender Endpoint Security Tools user interface.

[“Scanning for Malware” \(p. 10\)](#)

Find out how to run scans for malware.

[“Updates” \(p. 16\)](#)

Find out about Bitdefender Endpoint Security Tools updates.

[“Events” \(p. 18\)](#)

Check the activity of Bitdefender Endpoint Security Tools.

[“Getting Help” \(p. 19\)](#)

Where to look and where to ask for help if something unexpected appears.

3. Conventions Used in This Guide

Typographical Conventions

Several text styles are used in the guide for an improved readability. Their aspect and meaning are presented in the table below.

Appearance	Description
documentation@bitdefender.com	E-mail addresses are inserted in the text for contact information.
"Using This Guide" (p. iv)	This is an internal link, towards some location inside the document.
filename	Files and directories are printed using monospaced font.
option	All the product options are printed using bold characters.
keyword	Important keywords or phrases are highlighted using bold characters.

Admonitions

The admonitions are in-text notes, graphically marked, bringing to your attention additional information related to the current paragraph.



Note

The note is just a short observation. Although you can omit it, the notes can provide valuable information, such as specific feature or a link to some related topic.



Important

This requires your attention and is not recommended to skip over it. Usually, it provides non-critical but significant information.

4. Request for Comments


Please write to tell us how you think this guide could be improved and help us provide you with the best documentation possible.

Let us know by sending an e-mail to documentation@bitdefender.com.

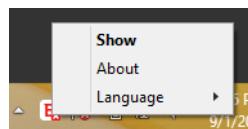
1. GETTING STARTED

Bitdefender Endpoint Security Tools is a fully-automated computer security program, managed remotely by your network administrator. Once installed, it protects you against all kinds of malware (such as viruses, spyware and trojans), network attacks, phishing and data theft. It can also be used to enforce your organization's computer and Internet use policies. Bitdefender Endpoint Security Tools will make most security-related decisions for you and will rarely show pop-up alerts. Details of actions taken and information about program operation are available in the **Events** area.

1.1. The System Tray Icon

At installation time, Bitdefender Endpoint Security Tools places an icon  in the system tray. If you double-click this icon, the main window will open. If you right-click the icon, a contextual menu will provide you with some useful options.

- **Show** - opens the main window of Bitdefender Endpoint Security Tools.
- **About** - opens a window with information about Bitdefender Endpoint Security Tools and states where to look for help in case of unexpected issues.
- **Language** - allows you to change the user interface language.
- **Power User** - allows you to access and modify security settings, after providing the password in the login window. Control Center is being notified when an endpoint is in Power User mode and the Control Center administrator can always overwrite local security settings.





System Tray Icon



Important

This option is available only if granted by the network administrator through policy settings.

The Bitdefender Endpoint Security Tools icon in the system tray informs you when issues affect your computer by changing the way it looks:


-  Critical issues affect the security of the system.
-  Some issues affect the security of the system.

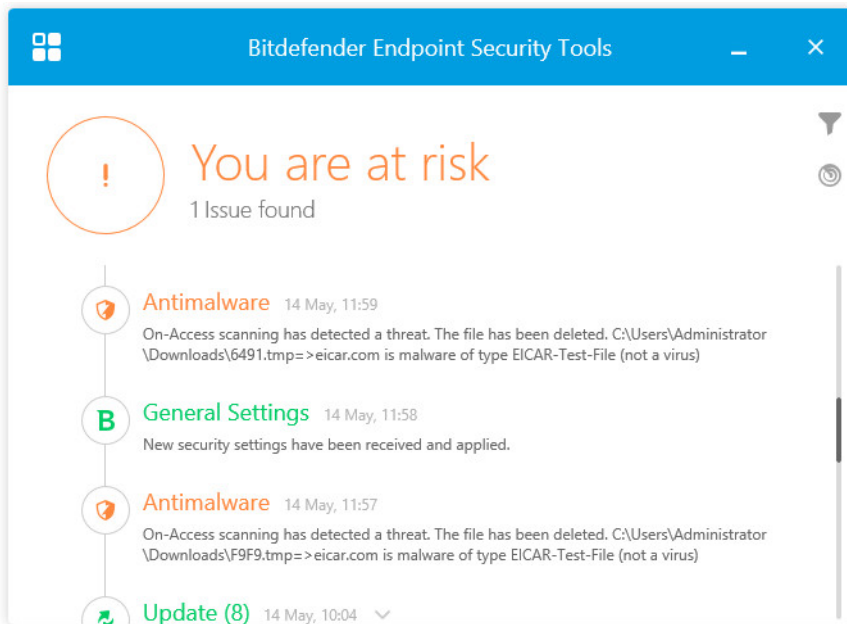
 **Note**

The network administrator can choose to hide the system tray icon.

1.2. The Main Window

The main window of Bitdefender Endpoint Security Tools allows you to check the protection status and perform scan tasks. Everything is just a few clicks away. Protection configuration and management are performed remotely by your network administrator.

To access the main interface of Bitdefender Endpoint Security Tools, use the Windows Start menu, by following the path **Start** → **All Programs** → **Bitdefender Endpoint Security Tools** → **Open Security Console** or, quicker, double-click the Bitdefender Endpoint Security Tools icon  in the system tray.



Main Window

The window is organized into two main areas:

- [Notifications area](#)

- [Events timeline](#)

1.2.1. The Notifications Area

The **Notifications** area offers useful information regarding the security of the system.



Notifications Area

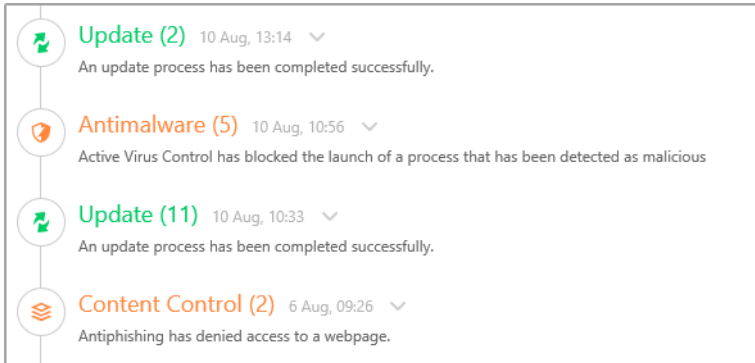
You can easily identify the current security status based on the status symbol displayed to the left of the notifications area:

- **Green check mark.** There are no issues to fix. Your computer and data are protected.
- **Yellow exclamation mark.** Non-critical issues are affecting the security of your system.
- **Red X mark.** Critical issues are affecting the security of your system.

In addition to the status symbol, a detailed security status message is displayed to the right of the notifications area. You can see the detected security issues by clicking inside the notifications area. Existing issues will be fixed by your network administrator.

1.2.2. Events Timeline


Bitdefender Endpoint Security Tools keeps a detailed log of events concerning its activity on your computer, including activities monitored by Content Control.

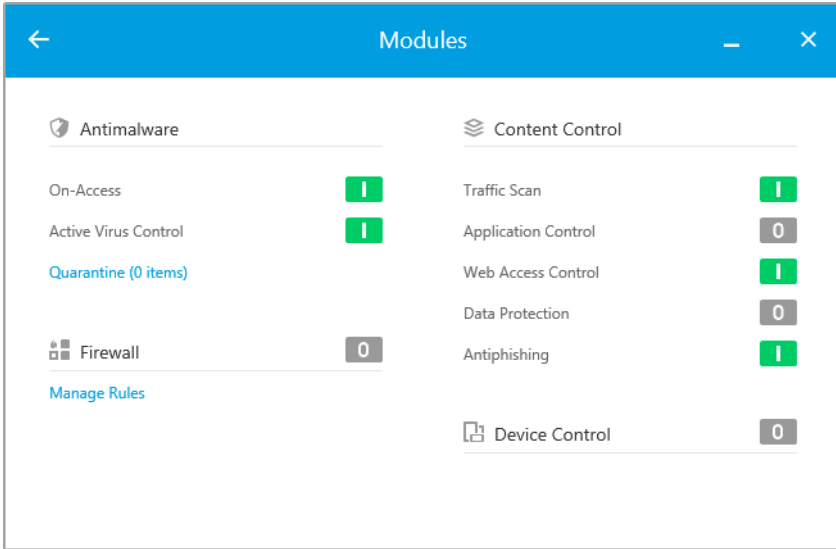


Events Timeline

The **Events** timeline is an important tool in monitoring your Bitdefender protection. For instance, you can easily check if an update was successfully performed or if malware was found on your computer. For more information, please refer to [“Events” \(p. 18\)](#).

1.3. The Modules Window

The **Modules** window displays useful information about the status and activity of the installed protection modules. To open the **Modules** window, click the **Modules** button  on the Bitdefender Endpoint Security Tools main window.

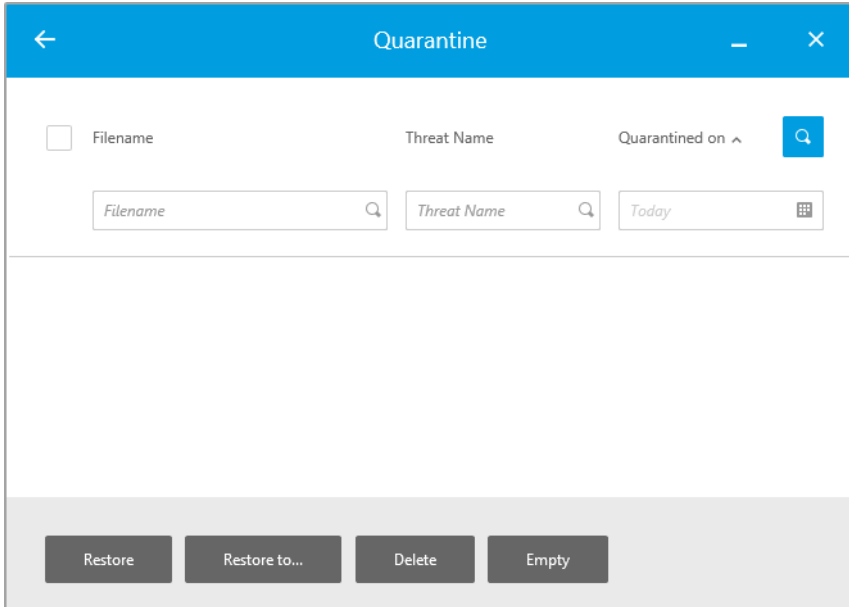


Modules Window

Antimalware

Antimalware protection is the foundation of your security. Bitdefender Endpoint Security Tools protects you in real time and on demand against all sorts of malware, such as viruses, trojans, spyware, adware, etc.

- **On-Access.** On-access scanning prevents new malware threats from entering the system by scanning local and network files when they are accessed (opened, moved, copied or executed), boot sectors and potentially unwanted applications (PUA).
- **Active Threat Control.** It continuously monitors applications running on the endpoint for malware-like actions. Active Threat Control will automatically try to disinfect the detected file.
- **Quarantine** displays the list of quarantined files, their original path, quarantine action time and date and their security status. Use the buttons at the bottom to delete or restore the files you want. If you want to delete all files from the quarantine, click the **Empty** button.



Quarantine

Content Control

The Content Control module protects you while on the Internet against phishing attacks, fraud attempts, private data leaks, and inappropriate web content. It also includes a comprehensive set of user controls that help the network administrator enforce computer and Internet use policies.

- **Traffic Scan.** This component prevents malware from being downloaded to the endpoint by scanning incoming emails and web traffic in real time. Outgoing emails are scanned to prevent malware from infecting other endpoints.
- **Application Control.** This component prevents access to unauthorized applications in your company. The administrator is responsible for creating rules for the allowed applications in the organization.
- **Web Access Control.** This component protects you from accessing dangerous websites based on administrator-defined rules. It also protects you against phishing.
- **Data Protection.** This component prevents unauthorized disclosure of sensitive data based on administrator-defined rules.

- **Antiphishing.** This component automatically blocks known phishing web pages to prevent users from inadvertently disclosing private or confidential information to online fraudsters.

Firewall


The firewall protects you while you are connected to networks and the Internet by filtering connection attempts and blocking suspicious or risky connections.

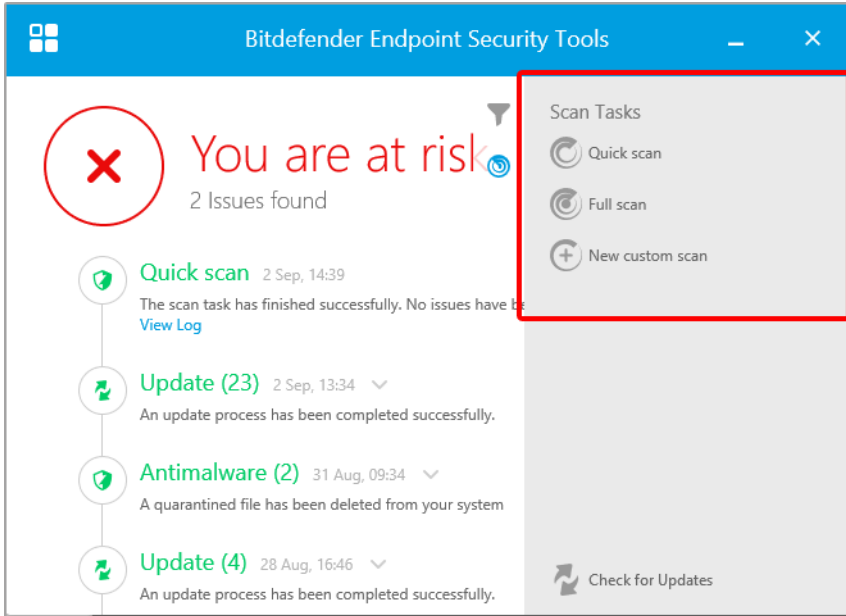
Device Control

It allows preventing sensitive data leakage and malware infections via external devices attached to endpoints, by applying blocking rules and exclusions via policy to a vast range of device types. The administrator is responsible for managing permissions for the following types of devices:

- Bluetooth Devices
- CDROM Devices
- Floppy Disk Drives
- IEEE 1284.4
- IEEE 1394
- Modems
- Security Policies 126
- Tape Drives
- Windows Portable
- COM/LPT Ports
- SCSI Raid
- Printers
- Network Adapters
- Wireless Network Adapters
- Internal and External Storage

1.4. Actions Menu

To define or run a scan task, click the **Actions** button  to open the **Actions** menu. This is where you can also check for updates.



Actions Menu

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 of a regular virus scan.

Full Scan

Checks the entire computer for all types of malware threatening its security, such as viruses, spyware, adware, rootkits and others.

Custom Scan

Allows you to choose the locations to scan and to configure scan options.



Check for updates

If an update is detected, you will be asked to confirm it or the update will be performed automatically, depending on the update settings configured by you network administrator.

2. SCANNING FOR MALWARE

The main objective of Bitdefender Endpoint Security Tools is to keep your computer free of malware. It does that primarily by scanning in real time accessed files, e-mail messages and any new files downloaded or copied to your computer. Besides real-time protection, it also allows running scans to detect and remove malware from your computer.

You can scan the computer whenever you want by running the default tasks or your own scan tasks (user-defined tasks). Scan tasks specify the scanning options and the objects to be scanned. If you want to scan specific locations on your computer or to configure the scan options, configure and run a custom scan.

At any point during the scan, you can see the progress in the **Events** timeline.

2.1. Scanning a File or Folder


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 Bitdefender Endpoint Security Tools**. The scan will start and you can monitor the progress on the **Events** timeline.

At the end of the scan, you will see the result. For detailed information, click **View Log**.

2.2. Running a 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.

To run a quick scan, follow these steps:

1. Open the Bitdefender Endpoint Security Tools window.
2. Click the **Actions** button  on the upper-right corner.
3. Click **Quick Scan**.
4. Wait for the scan to complete. You can see the progress of the scan in the timeline. Once complete, click **View Log** to see detailed results.

2.3. Running a Full Scan

The **Full Scan** task scans the entire computer for all types of malware threatening its security, such as viruses, spyware, adware, rootkits and others.



Note


Because **Full Scan** performs a thorough scan of the entire system, the scan may take a while. Therefore, it is recommended to run this task when you are not using your computer.

If you want to scan specific locations on your computer or to configure the scanning options, configure and run a custom scan. For more information, please refer to [“Configuring and Running a Custom Scan”](#) (p. 11).

Before running a full scan, the following are recommended:


- Make sure Bitdefender Endpoint Security Tools is up-to-date with its malware signatures. Scanning your computer using an outdated signature database may prevent Bitdefender Endpoint Security Tools from detecting new malware found since the last update. For more information, please refer to [“Updates”](#) (p. 16).

To run a full scan, follow these steps:


1. Open the Bitdefender Endpoint Security Tools window.
2. Click the **Actions** button  on the upper-right corner.
3. Click **Full Scan**.
4. Wait for the scan to complete. You can see the progress of the scan in the timeline. Click **View Details** to see the details of the scan in progress. You can also pause, postpone or stop the scan.
5. Bitdefender Endpoint Security Tools will automatically take the recommended actions on detected files. Once complete, click **View Log** to see detailed results.

2.4. Configuring and Running a Custom Scan

To configure a scan for malware in detail and then run it, follow these steps:

1. Open the Bitdefender Endpoint Security Tools main window.
2. Click the **Actions** button  on the upper-right corner.
3. Click **New Custom Scan**. The **Custom Scan** window will open.

4. Configure the scanning options: **Aggressive**, **Normal**, **Permissive**, **Custom**. Use the description below the option to identify the scan level that better fits your needs.
5. Select the target of the scan on the left-side pane.
6. You can also configure the scan to run the task with low priority by selecting the corresponding check box. This 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.

After configuring the custom scan, you can save it as a favourite. To do this, enter a name and click the **Favourite** button .

Advanced users might want to take advantage of the scan settings Bitdefender Endpoint Security Tools offers. To configure the scan options in detail, click **Custom** and then **Settings**.

2.4.1. File Types

On the **File types** tab, specify which types of files you want to be scanned. You can set the security agent to scan all files (regardless of their file extension), application files only or specific file extensions 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:

386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox;

rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm;
snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe;
vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf;
xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsx;
xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

Scan options for 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.

Scan email archives

Select this option if you want to enable scanning of email message files and email databases, including file formats such as .eml, .msg, .pst, .dbx, .mbx, .tbb and others.

2.4.2. What to Scan?

On the **Scan** tab, select the corresponding check boxes to enable the desired scan options.

Scan boot sectors

You can set Bitdefender Endpoint Security Tools 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 for rootkits

Select this option to scan for [rootkits](#) and objects hidden using such software.

Scan memory

Select this option to scan programs running in your system's memory.

Scan registry

Select this option to scan registry keys. Windows Registry is a database that stores configuration settings and options for the Windows operating system components, as well as for installed applications.

Scan cookies

Select this option to scan the cookies stored by browsers on your computer.

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.

2.4.3. What to Do?

On the **Actions** tab, set the action to be taken on the detected files, if any.

Infected files

Files detected as infected match a malware signature in the Bitdefender Malware Signature Database.

Suspect files

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

Rootkits

Rootkits represent specialized software used to hide files from the operating system. Though not malicious in nature, rootkits are often used to hide malware or to conceal the presence of an intruder into the system.

Take Proper Actions

Depending on the type of detected files, one or several of the following options are available:

Delete

Removes detected files from the disk.

If infected files are stored in an archive together with clean files, Bitdefender Endpoint Security Tools will attempt to delete the infected files and reconstruct the archive with the clean files. If archive reconstruction is not possible, you will be informed that no action can be taken so as to avoid losing clean files.

Ignore

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.

Move to quarantine

Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears.

Disinfect


Removes the malware code from the infected file and reconstruct the original file.

2.5. Checking 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 main window, once the scan is completed, by clicking **View Log**.

To check scan logs at a later time, follow these steps:

1. Open the Bitdefender Endpoint Security Tools main window.
2. Click the **Filter** button  to open the **Filters** menu.
3. Click the **Antimalware** button. Here you can find all malware scan events, including threats detected by on-access scanning, recent scans, user-initiated scans and status changes for automatic scans.
4. Click an event to view details about it.
5. To open the scan log, click **View Log**. The scan log will be displayed.

3. UPDATES

In a world where cyber criminals constantly try to come up with new ways to cause harm, having an up-to-date security program is essential if you are to stay one step ahead of them.

If you are connected to the Internet through broadband or DSL, Bitdefender Endpoint Security Tools takes care of this itself. By default, it checks for updates when you turn on your computer and every **hour** after that.



Note

The default automatic update frequency may be changed by your network administrator.

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.

If you are connected to the Internet through a dial-up connection, then it is recommended to regularly update Bitdefender by user request. For more information, please refer to [“Performing an Update”](#) (p. 17).

3.1. Types of Updates

Updates come in the following forms:

- **Updates for the malware signatures** - as new threats appear, the files containing malware signatures must be updated to ensure permanent up-to-date protection against them.
- **Product updates** - when a new product version is released, new features and scan techniques are introduced to the effect of improving the product's performance.

A product upgrade is a major version release.


3.2. Checking If Your Protection Is Up-to-Date

To check if your protection is up-to-date, follow these steps:

1. Right-click the Bitdefender Endpoint Security Tools icon **B** in the system tray and choose **About**.

2. You can see the update status and the time of the most recent update check and update installation.

For detailed information about the latest updates, check the update events:



1. In the main window, click the **Filter** button  to open the **Filters** menu.
2. Click the **Update** button. The latest updates will be displayed in the **Events** timeline.

You can see when updates were initiated and information about them - whether they were successful or not, if they require a restart to complete the installation. If required, restart the system at your earliest convenience.

3.3. Performing an Update

In order to perform updates, an Internet connection is required.

To start an update:

- Double-click the Bitdefender Endpoint Security Tools icon  in the **system tray**.
- Click the **Actions** button  to open the **Actions** menu.
- Click **Check for updates**. The Update module will connect to the Bitdefender update server and it will check for updates.
- If an update is detected, you will be asked to confirm it or the update will be performed automatically, depending on the update settings configured by you network administrator.




Important

If required, restart the system at your earliest convenience. We recommend doing it as soon as possible.




4. EVENTS

Bitdefender Endpoint Security Tools keeps a detailed log of events concerning its activity on your computer, including computer activities monitored by Content Control. The **Events** timeline is an important tool in monitoring your Bitdefender protection. For instance, you can easily check if an update was successfully performed, if malware was found on your computer etc. To check the events log, follow these steps:

1. Open the Bitdefender Endpoint Security Tools main window.
2. All events are displayed in the **Events** timeline.
3. Click the **Filter** button  to open the **Filters** menu.
4. Select the event category from the menu. Events are grouped into the following categories:
 - **General Settings**
 - **Antimalware**
 - **Firewall**
 - **Update**
 - **Content Control**
 - **Device Control**

Each event relates with the following information: a short description, the action Bitdefender took on it when it happened, and the date and time when it occurred. To see detailed information about a particular event in the list, click **View Log**.

You can also filter events by their importance to the protection level. There are three types of events:

-  indicates successful operations.
-  indicates non-critical issues.
-  indicates critical issues.



5. GETTING HELP

For any problems or questions concerning Bitdefender Endpoint Security Tools, please contact your network administrator.

To find product and contact information, right-click the Bitdefender Endpoint Security Tools icon **B** in the system tray and select **About** to open the **About** window.

Glossary

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.

Antivirus storm

An intensive use of system resources that occurs when antivirus software simultaneously scans multiple virtual machines on a single physical host.

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.

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.

Keylogger

A keylogger is an application that logs anything you type.

Keyloggers are not malicious in nature. They can be used for legitimate purposes, such as monitoring employees or children activity. However, they are increasingly being used by cyber-criminals for malicious purposes (for example, to collect private data, such as login credentials and social security numbers).

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.

Malware

Malware is the generic term for software that is designed to do harm - a contraction of 'malicious software'. It is not yet in universal usage, but its popularity as a general term for viruses, Trojan Horses, worms, and malicious mobile code is growing.

Malware signature

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

and detect malware. Signatures are also used to remove the malware code from infected files.

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

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.

Phishing

The act of sending an email 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 email 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. Bitdefender 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 email.

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 email 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.

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.

Bitdefender has its 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.

Worm

A program that propagates itself over a network, reproducing itself as it goes. It cannot attach itself to other programs.