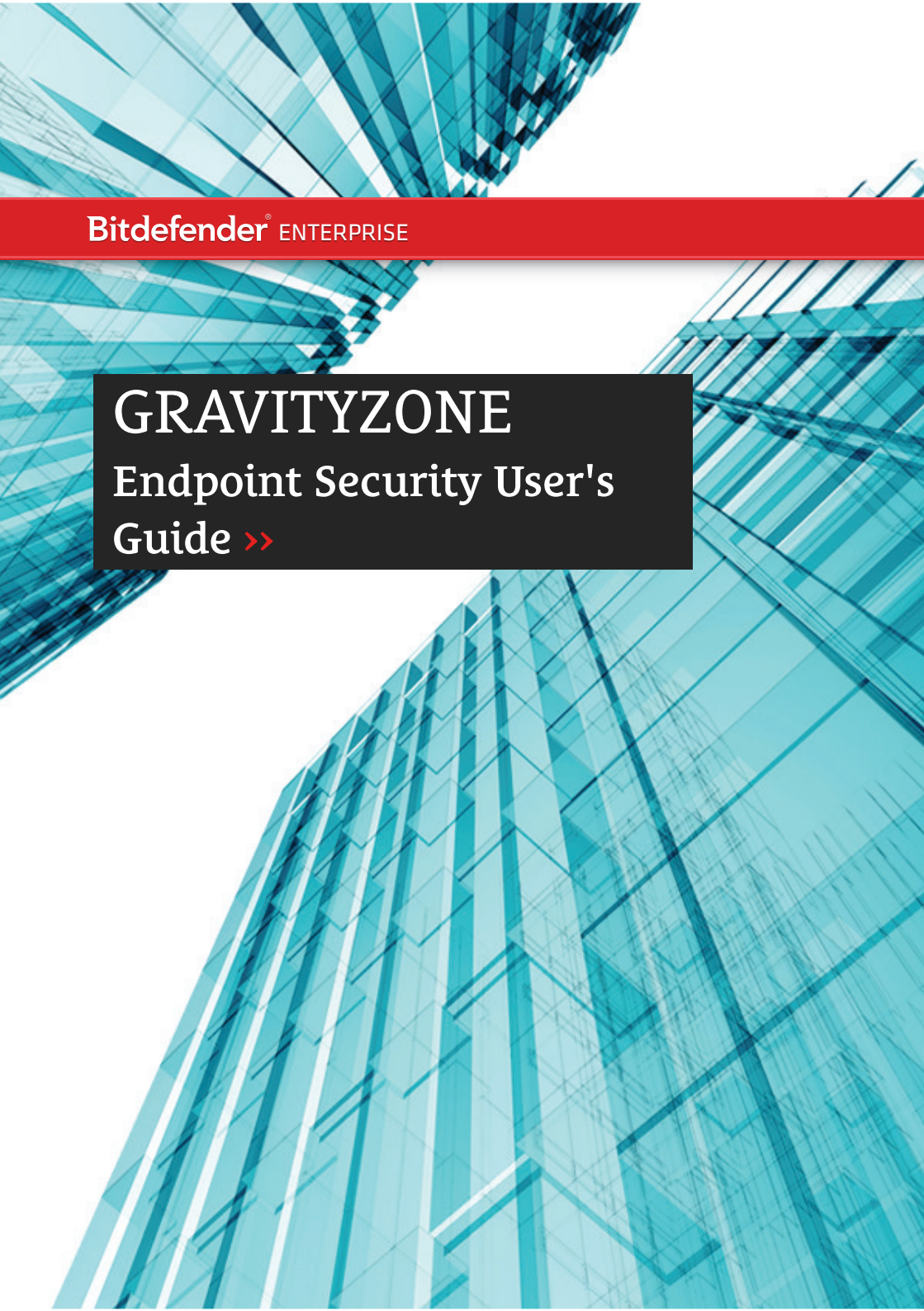

Bitdefender® ENTERPRISE
GRAVITYZONE
Endpoint Security User's Guide ››

GravityZone
Endpoint Security User's Guide

Publication date 2013.02.20


Bitdefender

Table of Contents

Using This Guide

1. Purpose and Intended Audience

This documentation is intended for the end users of **Endpoint Security**, 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.

We wish you a pleasant and useful lecture.

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 Endpoint Security user interface.

“Scanning for Malware” (p. 7)
Find out how to run scans for malware.

“Updates” (p. 14)
Find out about Endpoint Security updates.

“Events” (p. 16)
Check the activity of Endpoint Security.

“Getting Help” (p. 17)
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.

Appearance	Description
"Using This Guide" (p. v)	This is an internal link, towards some location inside the document.
`filename`	File 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

We invite you to help us improve the book. We have tested and verified all of the information to the best of our ability. Please write to tell us about any flaws you find in this book or how you think it could be improved, to help us provide you with the best documentation possible.

Let us know by sending an e-mail to documentation@bitdefender.com. Please write all of your documentation-related e-mails in English so that we can process them efficiently.

1. Getting Started

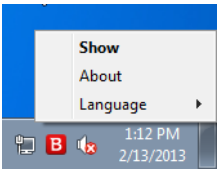
Endpoint Security is a fully-automated computer security program, managed remotely by your network administrator. Once installed, it protects you against all kinds of malware (such as viruses, spyware and trojans), network attacks, phishing and data theft. It can also be used to enforce your organization's computer and Internet use policies.

Endpoint Security will make most security-related decisions for you and will rarely show pop-up alerts. Details about actions taken and information about program operation are available in the Events window. For more information, please refer to “Events” (p. 16).

1.1. System Tray Icon

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

- **Show** - opens the main window of Endpoint Security.
- **About** - opens a window where you can see information about Endpoint Security and where to look for help in case something unexpected appears. Opening this window automatically initiates an on-demand update.
- **Language** - allows you to change the user interface language.



System Tray Icon

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

Critical issues affect the security of your system.

Non-critical issues affect the security of your system.

Note

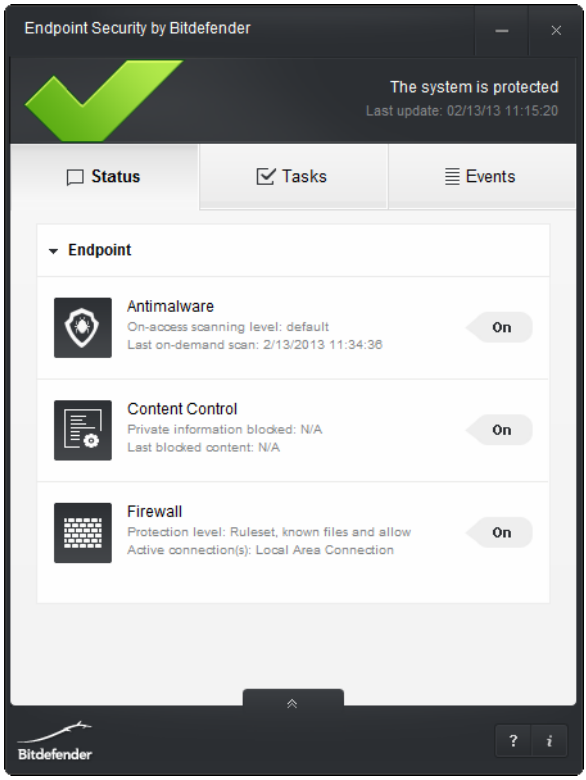
The network administrator can choose to hide the system tray icon.

1.2. Opening Main Program Window

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

1.3. Main Program Window

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

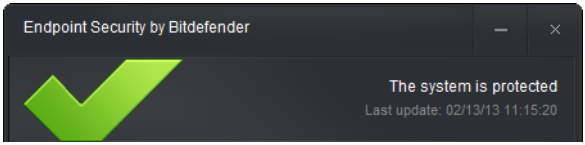


Main Program Window

The window is organized into two main areas:

Notification area

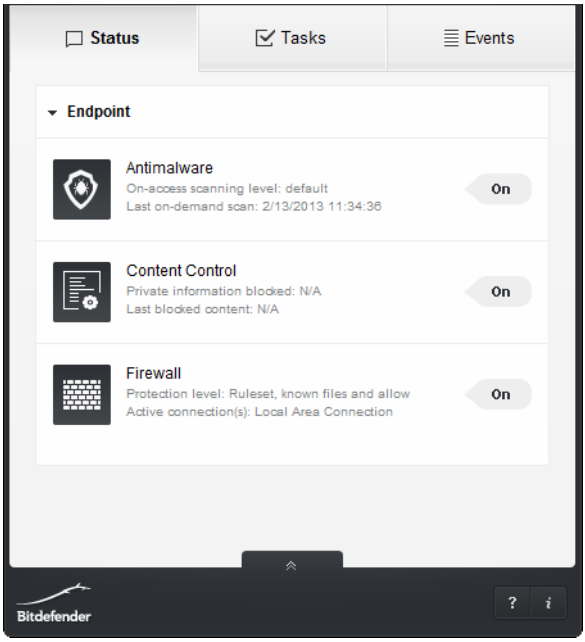
This is where you can check your computer's security status and see the issues affecting the security of your system.



Notification Area

Panels area

The panels area is where you can check the status of each installed protection module, manage the on-demand scan tasks and see the events logged by Endpoint Security.



Panels Area

Additionally, you can find useful support options on the lower part of the window:

Option	Description
?	Click this icon if you need help with Endpoint Security.
i	Click this icon to find product and contact information.

1.3.1. Notification Area

The notification area offers useful information regarding the security of the system.

You can easily identify the current security status based on the status symbol displayed to the left of the notification 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 exclamation 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 notification area. You can see the detected security issues by clicking anywhere inside the notification area. Existing issues will be fixed by your network administrator.

1.3.2. Panels Area

The panels area is where you can check the status of each installed protection module, manage the on-demand scan tasks and see the events logged by Endpoint Security.

The panels available in this area are:

Status

This is where you can view useful information about the status and activity of the installed protection modules.

- **Antimalware.** Antimalware protection is the foundation of your security. Endpoint Security protects you in real-time and on-demand against all sorts of malware, such as viruses, trojans, spyware, adware, etc.
- **Firewall.** The firewall protects you while you are connected to networks and the Internet by filtering connection attempts and blocking suspicious or risky connections.
- **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.

Tasks

This is where you can start system scans. You can run one of the following scan tasks:

- **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.
- **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 be scanned and to configure the scan options.

For information, refer to “Scanning for Malware” (p. 7).

Events

This is where you can access a detailed history of relevant events that occurred in the activity of the product. For detailed information, refer to “Events” (p. 16).

1.4. Web Browsing Protection

Your Security for Endpoints administrator may configure security settings that impact your web browsing experience. These security settings may pertain to:

- “Bitdefender Toolbar” (p. 5)
- “Search Advisor” (p. 5)
- “Blocked Web Pages” (p. 6)

1.4.1. Bitdefender Toolbar

When set by your Security for Endpoints administrator, the Bitdefender toolbar informs you about the security ratings of the web pages you are viewing. The Bitdefender toolbar is not your typical browser toolbar. The only thing it adds to the browser is a small dragger at the top of every web page. Clicking the dragger opens the toolbar.

Depending on how Bitdefender classifies the web page, one of the following messages is displayed on the toolbar:

- "This page is not safe" appears next to a red exclamation mark.
- "Caution is advised" appears next to an yellow exclamation mark.
- "This page is safe" appears next to a green check mark.

1.4.2. Search Advisor

When set up by your Security for Endpoints administrator, Search Advisor rates the results of Google, Bing and Yahoo! searches, as well as links from Facebook and Twitter, by placing an icon in front of every result. Icons used and their meaning:

You should not visit this web page.

This web page may contain dangerous content. Exercise caution if you decide to visit it.

This page could not be verified by Endpoint Security.

This is a safe page to visit.

1.4.3. Blocked Web Pages

Depending on the security policies set up by your Security for Endpoints administrator, specific web browsing protection settings against phishing and Internet frauds may be in place. Security for Endpoints may automatically block known phishing (website forgery/spoofing) web pages to prevent you from inadvertently disclosing private or confidential information to online fraudsters. In addition to website forgery, other types of Internet frauds may be suppressed such as: purchase frauds, get-rich-quick scams, Internet marketing frauds, click frauds, etc. Instead of the malicious web page, a special warning page is displayed in the browser to inform you that the requested web page is dangerous.

Note
If you need to access a legitimate web page that is incorrectly detected and blocked, please contact your Security for Endpoints administrator to set up an override.

1.5. Device Scanning

Endpoint Security may be configured to automatically detect storage devices (CDs/DVDs, USB storage devices or mapped network drives) and prompt you whether to scan them or not. The alert window provides you with information about the detected device.

To scan the device, click **Yes**. If you are sure the device is clean, you can choose not to scan it.

Note
If several devices are detected at the same time, alert windows are displayed, one at a time, for each of them.

Your Security for Endpoints administrator can choose to suppress Endpoint Security alerts and pop-ups. In such cases, the device scan is started automatically, without bothering you about it.

Whenever a device scan is running, a corresponding scan progress icon appears in the system tray. You can double-click this icon to open the scan window and to see the scan progress. You can pause or stop the device scan at any time. For more information, refer to “Antivirus Scan Wizard” (p. 10).

1.6. Changing Protection Settings

Endpoint Security is configured and managed remotely by your network administrator. You cannot change the protection settings.

Should you have questions concerning your protection settings, please address them to the person in charge with your network security.

2. Scanning for Malware

The main objective of Endpoint Security 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.

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 Endpoint Security by Bitdefender**. The Antivirus Scan wizard will appear and guide you through the scanning process. At the end of the scan, you will be prompted to choose the actions to be taken on the detected files, if any.

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 Endpoint Security window.
2. Go to the **Tasks** panel.
3. Click the **Scan** corresponding to the **Quick Scan** option.
4. Wait for the Antivirus Scan wizard to complete the scan. Endpoint Security will automatically take the recommended actions on detected files. If there remain unresolved threats, you will be prompted to choose the actions to be taken on them.

2.3. Running a Full System Scan

The Full System 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 System 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. 8).

Before running a Full System Scan, the following are recommended:

- Make sure Endpoint Security is up-to-date with its malware signatures. Scanning your computer using an outdated signature database may prevent Endpoint Security from detecting new malware found since the last update. For more information, please refer to "Updates" (p. 14).
- Shut down all open programs.

To run a Full System Scan, follow these steps:

1. Open the Endpoint Security window.
2. Go to the **Tasks** panel.
3. Click the **Scan** corresponding to the **Full Scan** option.
4. Wait for the Antivirus Scan wizard to complete the scan. Endpoint Security will automatically take the recommended actions on detected files. If there remain unresolved threats, you will be prompted to choose the actions to be taken on them.

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 Endpoint Security window.
2. Go to the **Tasks** panel.
3. Click the **New** corresponding to the **Custom Scan** option.

   A new window will appear. Follow these steps:

   a. 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.

      Advanced users might want to take advantage of the scan settings Endpoint Security offers. To configure the scan options in detail, click **Settings**. After selecting the desired custom settings the scan level will be automatically set to **Custom**. You can find information about the custom settings at the end of this section.

   b. 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 scan progress icon to open it.

4. Click **Next** to select the locations to be scanned.
5. Click the **Add** button to select the locations to be scanned. If you want to clear the target list, click the **Delete** button.
6. Click **Next** to start the scan and wait for the Antivirus Scan wizard to complete the scan. Depending on the locations to be scanned, the scan may take a while. At the end of the scan, you will be prompted to choose the actions to be taken on the detected files, if any.

Information on the scan options

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.
- **File types.** You can set Endpoint Security to scan all types of files or applications (program files) only. 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; xlsm; 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.

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

- **Scan boot sectors.** You can set Endpoint 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 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.
- **Ignore commercial keyloggers.** Select this option if you have installed and use commercial keylogger software on your computer. Commercial keyloggers are legitimate computer monitoring software whose most basic function is to record everything that is typed on the keyboard.

2.5. Antivirus Scan Wizard

Whenever you initiate an on-demand scan (for example, right-click a folder and select **Scan with Endpoint Security by Bitdefender**), the Endpoint Security Antivirus Scan wizard will appear. Follow the wizard 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 double-click this icon to open the scan window and to see the scan progress.

2.5.1. Step 1 - Perform Scan

Endpoint Security will start scanning the selected objects. You can see real-time information about the scan status and statistics (including the elapsed time, an estimation of the remaining time and the number of detected threats). To see more details, click the **Show more** link.

Wait for the scan to finish. The scanning process may take a while, depending on the complexity of the scan.

Stopping or pausing the scan. You can stop scanning anytime you want by clicking **Cancel**. 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.

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:

- **Password.** If you want Endpoint 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.
- **Don't ask for a password and skip this object from scan.** Select this option to skip scanning this archive.
- **Skip all password-protected items without scanning them.** Select this option if you do not want to be bothered about password-protected archives. Endpoint Security will not be able to scan them, but a record will be kept in the scan log.

Choose the desired option and click **OK** to continue scanning.

2.5.2. Step 2 - Choose Actions

At the end of the scan, you will be prompted to choose the actions to be taken on the detected files, if any.

Note

When you run a Quick Scan or a Full System Scan, Endpoint Security will automatically take the recommended actions on detected files during the scan. If there remain unresolved threats, you will be prompted to choose the actions to be taken on them.

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 proper actions

Endpoint Security will take the recommended actions depending on the type of detected file:

- **Infected files.** Files detected as infected match a malware signature in the Bitdefender Malware Signature Database. Endpoint 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. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears.

  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.

- **Suspicious files.** Files are detected as suspicious by the heuristic analysis. Suspicious files cannot be disinfected, because no disinfection routine is available. They will be moved to quarantine to prevent a potential infection.

  By default, quarantined files are automatically sent to Bitdefender Labs in order to be analyzed by the Bitdefender malware researchers. If malware presence is confirmed, a signature is released to allow removing the malware.

- **Archives containing infected files.**
  - Archives that contain only infected files are deleted automatically.
  - If an archive contains both infected and clean files, Endpoint Security will attempt to delete the infected files provided it can 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 loosing clean files.

Delete

Removes detected files from the disk.

If infected files are stored in an archive together with clean files, Endpoint Security 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 loosing 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.

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

2.5.3. Step 3 - Summary

When Endpoint 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.

Click **Close** to close the window.

Important

In most cases Endpoint Security successfully disinfects the infected files it detects or it isolates the infection. However, there are issues that cannot be solved automatically. If required, please restart your system in order to complete the cleaning process.

2.6. 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 scan wizard, once the scan is completed, by clicking **Show Log**.

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

1. Open the Endpoint Security window.
2. Go to the **Events** panel.
3. Select **Antimalware** in the second menu. This is where you can find all malware scan events, including threats detected by on-access scanning, user-initiated scans and status changes for automatic scans.
4. In the events list, you can check what scans have been performed recently. Click an event to view details about it.
5. To open the scan log, click the location mentioned in the details area at the bottom of the panel. 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, Endpoint 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, it is automatically downloaded and installed on your computer.

Note

The default automatic update frequency may be changed by your network administrator. For more information, please refer to "What Is the Automatic Update Frequency?" (p. 15).

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. 15).

3.1. Types of Updates

Updates come in the following ways:

- **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 icon  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, go to the **Events** panel.
2. Click **Update** in the second menu.

You can find out 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, right-click the Bitdefender icon in the system tray and choose **About**. Opening the **About** window automatically initiates an on-demand update.

The Update module will connect to the Bitdefender update server and it will check for updates. If an update is detected, it is automatically downloaded and installed on your computer.

Important
It may be necessary to restart the computer when you have completed the update. We recommend doing it as soon as possible.

3.4. What Is the Automatic Update Frequency?

Endpoint Security automatically checks for updates when you turn on your computer and every **hour** after that.

4. Events

Endpoint Security keeps a detailed log of events concerning its activity on your computer (also including computer activities monitored by Content Control). Events are a very important tool in monitoring your Bitdefender protection. For instance, you can easily check if the update was successfully performed, if malware was found on your computer etc.

To check the events log, follow these steps:

1. Open the Endpoint Security window.
2. Go to the **Events** panel.
3. Select the event category from the second menu. Events are grouped into the following categories:
   - **Antimalware**
   - **Content Control**
   - **Update**
   - **Firewall**
   - **General**

A list of events is available for each category. To find out information about a particular event in the list, click it. Event details are displayed in the lower part of the window. Each event comes with the following information: a short description, the action Bitdefender took on it when it happened, and the date and time when it occurred.

You can filter events by their importance. There are three types of events:

Information events indicate successful operations.

Warning events indicate non-critical issues.

Critical events indicate critical issues.

Events can only be deleted by your network administrator.

5. Getting Help

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

To find product and contact information, do any of the following:

- Open the Endpoint Security window and click the **Info** icon in the bottom-right corner.
- Right-click the Bitdefender icon in the system tray and choose **About**.

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.

Email

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.

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.

Mail client

An email client is an application that enables you to send and receive email.

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.

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 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.

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.

Bitdefender 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.

Worm

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