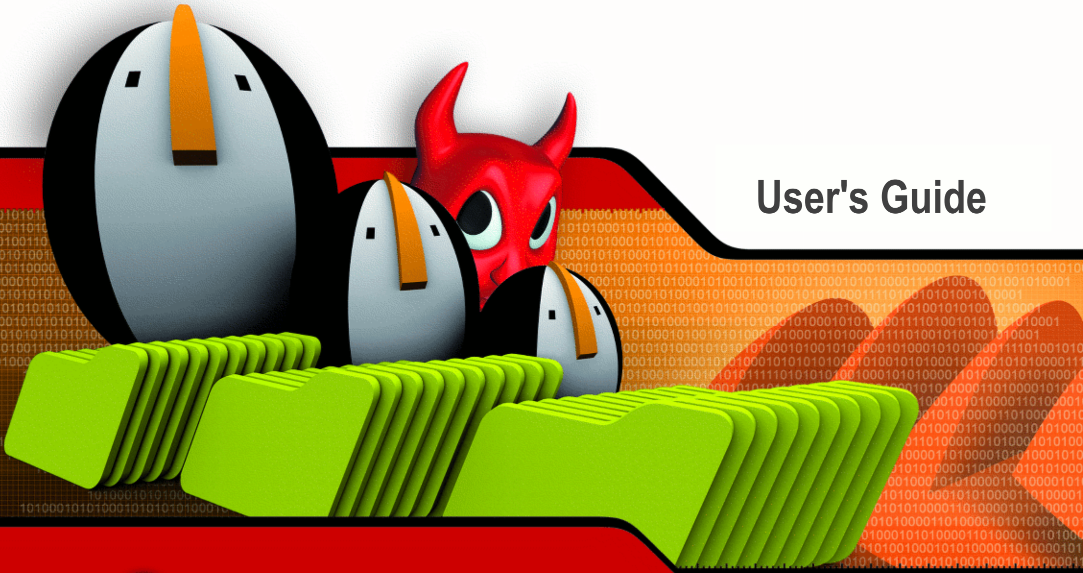
bitdefender®



User's Guide

antivirus

Antivirus scanner for Unices

BitDefender Antivirus Scanner for Unices
User's Guide

BitDefender

Publication date 2012.06.19
Revision Version 1.24.1960

Legal Notice

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

End User Software License Agreement

IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS DO NOT INSTALL THE SOFTWARE. BY SELECTING "I ACCEPT", "OK", "CONTINUE", "YES" OR BY INSTALLING OR USING THE SOFTWARE IN ANY WAY, YOU ARE INDICATING YOUR COMPLETE UNDERSTANDING AND ACCEPTANCE OF THE TERMS OF THIS AGREEMENT.

These Terms cover the home-user or corporate BitDefender Solutions and Services licensed to you, including the related documentation and any update and upgrade of the applications delivered to you under the purchased license or under any related service agreement, as defined in the documentation, as well as any copy thereof.

This License Agreement is a legal agreement between you (either an individual or a legal person) and BitDefender for the use of the BitDefender software product identified above, which includes computer software and services, and may include the associated media, printed materials, and "online" or electronic documentation (hereinafter referred to as "BitDefender"), all of which are protected by international copyright laws and international treaties. By installing, copying or using BitDefender, you agree to be bound by the terms of this agreement.

If you do not agree to the terms of this agreement, do not install or use BitDefender.

BitDefender License. BitDefender is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. BitDefender is licensed, not sold.

GRANT OF LICENSE. BitDefender hereby grants you and only you the following non-exclusive, limited, non-transferable and royalty-bearing license to use BitDefender.

The BitDefender Antivirus Scanner for Unices ("BitDefender") is subject to 3 types of license:

1. Trial License. The product is distributed with a trial key which grants the user a 30 day trial period as of install time, under the terms of the license agreement. At the end of the trial period, all scan- based product features (disinfect, delete) will be disabled and the user will have to either go online to www.bitdefender.com and register for a personal license or purchase a commercial license from any BitDefender reseller.

2. Home or Personal Use License. This license is free of charge and it can be retrieved from the BitDefender website after filling in a short form. It only allows the product to be used for personal purposes, with no commercial implications whatsoever, under the terms of the EULA. For example, under the Personal License, you are allowed to scan your personal laptop or desktop computer but YOU ARE NOT ALLOWED TO USE THE PRODUCT IN A BUSINESS ENVIRONMENT SUCH AS AN OFFICE COMPUTER OR A COMPANY SERVER.

3. Commercial Use License. If you intend to use BitDefender with your own integration system or pre-designed scripts, you must purchase the Commercial License. The commercial license allows for the product to be used in any environment whatsoever throughout the licensing period, under the terms of the EULA. Commercial Licenses are granted on an individual user basis, which simply means that the cost depends on how many users benefit from the features of the product.

LICENSE TERM. The license hereunder is granted as of the date BitDefender has been purchased and until the end of the period for which such license has been purchased.

UPGRADES. If BitDefender is upgrade labeled, in order to use it, you must hold a BitDefender license allowing you to use products identified by such company as eligible for upgrade. An upgrade labeled BitDefender product shall replace and/or supplement the product based on which your were eligibile for such upgrade. You may use the resulting upgraded product only in accordance with the terms of this License Agreement. If BitDefender is an upgrade of a software package component which was licensed to you as a single product, BitDefender may only be used and transferred as part of that single product package and it may not be separated so as to be used by more than the total number of licensed users. The terms and conditions of this license shall replace and supersede any previous agreements that may have existed between you and BitDefender regarding the original product or the resulting upgraded product.

COPYRIGHT. All rights, titles and interest in and to BitDefender and all copyrights in and to BitDefender (including but not limited to any images, photographs, logos, animations, video, audio, music, text, and "applets" incorporated into BitDefender), the accompanying printed materials, and any copies of BitDefender are property of BitDefender. BitDefender is protected by copyright laws and international treaty provisions. Therefore, BitDefender must be treated as any other copyrighted material. The printed materials accompanying BitDefender shall not be copied. All copyright notices shall be reproduced and included, in their original form, in all of the BitDefender copies created, irrespective of the media or form in which BitDefender exists. The BitDefender license shall not be sub-licensed, rented, sold, leased or shared. The BitDefender source code shall not be reverse engineered, recompiled, disassembled, no derivative works shall be created based on it, it shall not be modified, translated and no attempts to discover it shall be made.

LIMITED WARRANTY. BitDefender warrants a 30 day fault free period for the media on which BitDefender is distributed as of the date BitDefender has been delivered to you. Any breach of this warranty shall only result in BitDefender replacing the faulty media, at its sole discretion, upon receipt of the said media, or refunding the BitDefender price. BitDefender does not warrant either the uninterrupted or error free operation of BitDefender or the correction of possible errors. BitDefender does not warrant that BitDefender will meet your requirements.

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, BitDefender DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE PRODUCTS, ENHANCEMENTS, MAINTENANCE THEREOF OR SUPPORT RELATED THERETO, OR ANY OTHER MATERIALS (TANGIBLE OR INTANGIBLE) OR SERVICES THAT IT HAS SUPPLIED. BitDefender HEREBY EXPRESSLY DISCLAIMS ANY IMPLIED WARRANTIES AND CONDITIONS, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INTERFERENCE, ACCURACY OF DATA, ACCURACY OF INFORMATIONAL CONTENT, SYSTEM INTEGRATION, AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS BY FILTERING, DISABLING, OR REMOVING SUCH THIRD PARTY'S SOFTWARE, SPYWARE, ADWARE, COOKIES, EMAILS, DOCUMENTS, ADVERTISEMENTS OR THE LIKE, WHETHER ARISING BY STATUTE, LAW, COURSE OF DEALING, CUSTOM AND PRACTICE, OR TRADE USAGE.

DISCLAIMER OF DAMAGES. Anyone using, testing, or evaluating BitDefender shall bears all risks as to the quality and performance of BitDefender. Under no circumstances shall BitDefender be liable for any damages of any kind, including, without limitation, direct or indirect damages arising out of the use, performance, or delivery of BitDefender, even if BitDefender has been advised of the existence or possibility of such damages.

SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

UNDER NO CIRCUMSTANCES SHALL BitDefender'S LIABILITY EXCEED THE PURCHASE PRICE PAID BY YOU FOR BITDEFENDER. The disclaimers and limitations set forth above shall apply regardless of whether you accept to use, evaluate, or test BitDefender.

IMPORTANT NOTICE TO USERS. THIS SOFTWARE IS NOT FAULT-TOLERANT AND IT IS NOT DESIGNED OR INTENDED FOR USE IN ANY HAZARDOUS ENVIRONMENT REQUIRING FAIL-SAFE PERFORMANCE OR OPERATION. THIS SOFTWARE IS NOT INTENDED FOR USE IN THE OPERATION OF AIRCRAFT

NAVIGATION, NUCLEAR FACILITIES, OR COMMUNICATION SYSTEMS, WEAPONS SYSTEMS, DIRECT OR INDIRECT LIFE-SUPPORT SYSTEMS, AIR TRAFFIC CONTROL, OR ANY APPLICATION OR INSTALLATION WHERE FAILURE COULD RESULT IN DEATH, SEVERE PHYSICAL INJURY OR DAMAGE TO PROPERTY.

GENERAL. This Agreement shall be governed by the Romanian law and by the international copyright regulations and treaties. The courts of Romania shall have exclusive jurisdiction and venue to adjudicate any dispute arising from these License Terms.

BitDefender prices, costs and use fees are subject to change without prior notice to you.

In the event of invalidity of any provision of this Agreement, the invalidity shall not affect the validity of the remaining portions of this Agreement.

BitDefender and the BitDefender logos are trademarks of BitDefender. All other trademarks used in the product or in associated materials are property of their respective owners.

Any breach of these terms and conditions shall result in the immediate termination of this license, without any notice. You shall not be entitled to a refund from BitDefender or any resellers of BitDefender as a result of such termination. Confidentiality terms and conditions and restrictions on use shall remain in force even after termination.

BitDefender may revise these Terms at any time and the revised terms shall automatically apply to the corresponding versions of the Software distributed under such terms. None of these Terms being found to be void and unenforceable shall affect the validity of rest of the Terms, which shall remain valid and enforceable.

In case of controversy or inconsistency between the translations of these Terms into other languages, the English version issued by BitDefender shall prevail.

Contact BitDefender at West Gate Park, Building H2, 24 Preciziei Street, Sector 6, Bucharest, Romania, or at Tel No: +40 21 2063470, e-mail address: <office@bitdefender.com>.

Preface

This *User's Guide* is intended for all those who have chosen to use BitDefender Antivirus Scanner for Unices as a security solution for their systems. The information presented in this book is suitable not only for computer literates, but also for anyone who can do administrative tasks on a Linux or FreeBSD system.

This book will describe for you BitDefender Antivirus Scanner for Unices, will guide you through the installation process, will teach you how to configure it in detail. You will find out how to use, update, interrogate, test and customize BitDefender Antivirus Scanner for Unices. You will also learn how to integrate it with various software and how to get the best from BitDefender.

We hope this will be a pleasant and useful reading.

1. Conventions Used in This Book

1.1. Typographical Conventions

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

Appearance	Description
`variable`	Variables and some numerical data are printed in `monospaced` characters.
http://www.bitdefender.com	The URL link is pointing to some external location, on http or ftp servers.
`<support@bitdefender.com>`	E-mail addresses are inserted in the text for contact information.
Chapter 4 "*Installation*" (p. 15)	This is an internal link pointing towards a location inside the document.
`filename`	File and directory names are printed in a `monospaced` font.

Appearance	Description
`ENV_VAR`	Environment variables are printed in `MONOSPACED CAPITALS`.
emphasized	*Emphasized texts* are especially marked to draw your attention.
“quoted text”	Quoted texts are provided as reference.
command	Inline commands are printed in **strong** characters.
`# command -parameter`	Command examples are printed in strong monospaced characters within a specially marked environment. The prompt can be one of the following: **#** Root prompt. You should be root in order to run this command. **$** Normal user prompt. You do not need special privileges to run this command.
`screen output`	The screen output and code listings are printed in monospaced characters within a specially marked environment.

1.2. Admonitions

Admonitions are graphically marked, in-text notes drawing your attention to additional information related to the respective paragraph.

Note
A note is just a short observation. Although you can omit it, a note can provide valuable information, such as specific features or a link to a related topic.

Important
This is information which requires your attention and should not be skipped. It usually is non-critical, but significant information.

Warning
This is critical information you should treat with increased caution. Nothing bad will happen if you follow the directions. You should read and understand the warning, because it describes something extremely risky.

2. Book Structure

The book consists of several parts covering several major topics: Description, Installation and Removal, Command Line Interface Scanner, Graphical User Interface Scanner and Getting Help. Moreover, a glossary and UNIX manual pages are provided to clarify different aspects of BitDefender, which might raise technical issues.

Description. A short introduction to BitDefender Antivirus Scanner for Unices. You are presented with the BitDefender Antivirus Scanner for Unices, its features, the product components (bdscan, bdgui) and the basics of the integration, filtering mechanism and graphical interface.

Installation and Removal. Step-by-step instructions on how to install BitDefender Antivirus Scanner for Unices on a system. Starting with the prerequisites of a successful installation, you are guided through the entire installation process. Finally, the uninstall procedure is described in case you need to uninstall BitDefender.

Command Line Interface Scanner. Description of the administration and usage of the command line interface scanner. This is a presentation of the BitDefender configuration file and of how to get run-time information, test the antivirus efficiency, perform updates and register the product. You are also presented real life usage scenarios, covering various aspects: detecting malware on your system, several desktop and e-mail server integration procedures, setting the antivirus to scan files directly from the file manager or the e-mail passing through your local e-mail server. Manual pages are included for quick and convenient reference. Whenever you find examples of commands in BitDefender Antivirus Scanner for Unices, the manual pages will provide you with valuable help in understanding all the options and actions.

Graphical User Interface Scanner. Description of the administration and usage of the graphical user interface scanner. This is a presentation of how to configure the antivirus scanning, perform updates and register the product.

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

Glossary. The Glossary tries to explain some technical and uncommon terms you will find in the pages of this book.

3. 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, but you may find that features have changed (or even that we have made mistakes). 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 your opinions and suggestions by sending an e-mail at <documentation@bitdefender.com>.

Note

You can find out the latest by visiting the BitDefender Unix blog at http://unices.bitdefender.com/.

Description and Features

1. Product Features

Purchasing and installing an antivirus product for your personal or your company's systems is the most efficient way of preventing the infection of a computer and the spreading of viruses inside and outside the network it is connected to.

BitDefender Antivirus Scanner for Unices is the solution BitDefender offers for the antivirus protection of mixed networks. It uses the most advanced multi-platform virus inspection technology which scans for viruses and other malware on your personal system.

It consists of two major elements:

- A command line interface scanner (`bdscan`).
- A graphical user interface scanner (`bdgui`).

bdscan. The on-demand scanner, intended for command line or shell scripts, features manual scan of individual files or entire file systems, malicious code detection and removal. After each scan, the program displays a detailed report on positive virus detections. Thanks to the advanced features of the BitDefender scan engines, new, undiscovered threats can be detected and immediately eliminated from the system. All the files specified in the command line are scanned using the BitDefender scan engines. The scan engines detect all the viruses from common files, archives or mailboxes. BitDefender features built-in support for more than 80 packed files formats, including RAR, ZIP, ARJ, LZH, LHA, ACE, GZIP, TARGZ, JAR, UUE, MIME or CAB archives, no matter how they were created (self-extractable, multivolume, etc). If an infection is found, the file will be treated according to the selected option (disinfection, deletion, isolation in the quarantine area or just reporting) and notifications will be sent to the console, as well as to the log file. To ensure superior and efficient antivirus protection, BitDefender Antivirus Scanner for Unices was designed with a built-in update function.

bdgui. The graphical user interface scanner helps you scan your computer very easily. It allows you to configure the antivirus scanning in accordance with your needs, to perform updates and register the product.

2. CLI Scanning Mechanism

The central part of BitDefender Antivirus Scanner for Unices consists of the BitDefender architecture-independent scanning engines. These are specialized data analysis routines and malware signature definitions, since many viruses can be identified based on a distinctive code pattern.

To identify unknown viruses, the engines can perform a heuristic analysis, searching for several features characterizing viruses.

The objects to be scanned can be directories or regular files, provided as command line parameters.

The object submitted for scanning is unpacked, if needed, and scanned. The scanning result is sent back to **bdscan**, which will further notify the user and try to apply the desired action. The actions to be applied, triggered with the `--action` command line option, can be one of the following:

- **Disinfect.** BitDefender will try to disinfect the object by removing the infected or suspected part. The action can sometimes fail.
- **Quarantine.** The object will be moved from its original location to a secured directory, the Quarantine.
- **Delete.** The object will be simply removed from the filesystem.
- **Ignore.** Even if infected objects are found, BitDefender will just report them and no action will be performed.

By default, **bdscan** will scan inside archives, mail boxes and packed programs. If this behavior is not desirable, command line options are available for you to disable scan target types selectively `--no-archive`, `--no-mail` and `--no-pack`, respectively.

If the scanning path is a directory, **bdscan** will recursively descend in sub-directories and scan the files found. The recursion depth can be specified in a command line or it can be entirely disabled.

More Info

You can find out more about the supported command line options in the bdscan(8) manual page.

Installation and Removal

3. Prerequisites

BitDefender Antivirus Scanner for Unices can be installed on:

- Debian-based distributions, using deb packages.
- Red Hat-based distributions, using rpm packages.
- all the other Linux distributions, using a pseudo-package system (ipk packages).
- FreeBSD versions, using tbz packages (these packages are built as bzip2 compressed tars).

These packages include all the necessary pre-install, post-install, pre-remove and post-remove scripts. The adequate package type should be installed according to the distribution.

3.1. System Requirements

Before installing BitDefender Antivirus Scanner for Unices, you must verify that your system meets the minimum system requirements. The minimum requirements depend on whether you install only the command line interface (CLI) scanner or all of the product components (full installation).

3.1.1. CLI Scanner Installation

If you want to install only the command line interface scanner, your system must meet the following system requirements:

Hardware Requirements

Processor type

x86 compatible, minimum 166 MHz, but do not expect a great performance in this case. An i686 generation processor, at 300MHz, would make a better choice.

Memory

The minimum accepted value is 128 MB, but, for improved performance, the recommended value is 256 MB.

Free disk space

The minimum free disk space required to install and run BitDefender Antivirus Scanner for Unices is 64 MB. However, the log and the quarantine directories could require more space.

Internet connection

Although BitDefender Antivirus Scanner for Unices will run with no Internet connection, the update procedure will require an active HTTP link, even through a proxy server. Therefore, the Internet connection is a MUST to keep your protection up to date.

Software Requirements

Linux requirements

The supported Linux kernel versions are 2.2, 2.4 or 2.6, but the recommended one is 2.6.

BitDefender requires at least `glibc` version 2.3 and `libstdc++` from the `gcc 3.x` series.

FreeBSD requirements

The supported FreeBSD versions are 5.4-RELEASE and higher, and 6.0-RELEASE and higher.

FreeBSD 4 is no longer supported.

3.1.2. Full Installation

If you want to install both the command line interface scanner and the graphical user interface scanner, your system must meet the following system requirements:

Hardware Requirements

Processor type

x86 or amd64 compatible, 500MHz or higher.

Memory

The minimum accepted value is 128 MB. For improved performance, the recommended value is 256 MB.

Free disk space

The minimum free disk space required to install and run BitDefender Antivirus Scanner for Unices is 64 MB. However, the log and the quarantine directories could require more space.

Internet connection

Although BitDefender Antivirus Scanner for Unices will run with no Internet connection, the update procedure will require an active HTTP link, even through a proxy server. Therefore, the Internet connection is a MUST to keep your protection up to date.

Software Requirements

Linux requirements

The Linux kernel should be 2.4 or 2.6 (recommended).

BitDefender requires at least `glibc` version 2.6 and `libfontconfig` version 2.4.2.

FreeBSD requirements

The supported FreeBSD versions are 6.0-RELEASE and higher.

3.2. Package Naming Convention

The BitDefender Antivirus Scanner for Unices packages are included in self-extractable `.run` archives that respect the following naming convention:

```
BitDefender-Antivirus-Scanner-{ver}.{os}.{arch}.{pkg}.run
```

Note

The archive name may also contain the `nogui` string. This indicates that the archive does not contain the graphical user interface scanner.

Variable	Description
`{ver}`	This is the package version. For example, 7.5-3 is version 7, subversion 5, package build 3.
`{os}`	This is the operating system identifier. It indicates that the package can be installed on a Linux distribution compiled with a specific version of the gcc compiler (for example,

Variable	Description
	linux-gcc4x) or on a specific version of FreeBSD (for example, freebsd6).
{arch}	This specifies the processor architecture. i586 is the current development version.
{pkg}	This refers to the package management tool used to install the files. This may be rpm, deb, ipk or tbz. • rpm uses the Red Hat Package Manager. • deb uses the Debian package system. • ipk is a generic packaging system, a portable method for systems that do not use deb and rpm. • tbz is used for FreeBSD. Please install the appropriate package for your system, as described in the next sections.

The naming convention for the self-extactable .run archive is the same, regardless of whether the archive includes the packages for a Linux distribution or for FreeBSD. However, the naming convention of the packages depends on the operating system they are to be installed on.

3.2.1. Linux Convention

Linux packages are named according to the following conventions:

Debian (.deb) and generic (.ipk) packages

- Command line interface scanner package:

```
bitdefender-scanner_{ver}.{arch}.{pkg}
```

- Graphical user interface scanner package:

```
bitdefender-scanner-gui_{ver}.{arch}.{pkg}
```

Red Hat (.rpm) packages

- Command line interface scanner package:

```
bitdefender-scanner-{ver}.{arch}.rpm
```

- Graphical user interface scanner package:

```
bitdefender-scanner-gui-{ver}.{arch}.rpm
```

3.2.2. FreeBSD Convention

FreeBSD packages are named as follows:

- Command line interface scanner package:

```
bitdefender-scanner-{ver}.tbz
```

- Graphical user interface scanner package:

```
bitdefender-scanner-gui-{ver}.tbz
```

{ver} is the package version. For example, 7.6.3 is version 7, subversion 6, package build 3.

4. Installation

This section explains how to install BitDefender Antivirus Scanner for Unices on Linux or FreeBSD systems. This is pretty straightforward: get the appropriate package, test it for integrity, then install it.

4.1. Get BitDefender Antivirus Scanner for Unices

The package can be downloaded from the BitDefender servers or it can be found on different distribution media, such as CD-ROMs. When downloading from the BitDefender servers, you will be asked to fill in a form and you will receive an e-mail at the address you provided in this form. The email contains the download location.

Linux packages come in three flavours:

- `rpm` for distributions using the Red Hat Linux package manager
- `deb` for distributions using the Debian Linux packaging system
- `ipk`, a generic packaging system, a portable method for Linux systems that do not use deb and rpm

The FreeBSD package is a tbz (.tar.bz2) compressed archive. There is one package for FreeBSD 5 (only the command line interface scanner is supported) and there are two packages for FreeBSD 6 (one for the CLI scanner and one for the GUI scanner).

These packages are included in self-extractable archives with the `.run`extension, which you can easily install.

4.2. Test Package Integrity

Before you begin the installation process, you should check the package to make sure it is not corrupted (this can happen sometimes, especially if you downloaded it).

4.2.1. Test Self-extractable Archive

To check the integrity of the self-extractable archive, run the following command and get the corresponding answer.

```
# sh BitDefender-Antivirus-Scanner-{ver}.{os}.{arch}.run --check
   Verifying archive integrity... MD5 checksums are OK. All good.
```

If you get a different answer (an error), please download the package again.

4.2.2. Test rpm and deb Packages

For increased security, `rpm` and `deb` packages are GPG signed. To test their integrity, you can verify their signature.

First, you need to fetch the **BitDefender Packages GPG key** (key id: `0x0EC4FE05`) from a key server, by running the following command:

```
# gpg --recv  --keyserver pgp.mit.edu 0x0EC4FE05
```

Then, export the key to a local file:

```
# gpg --armor --export 0x0EC4FE05  > bd-pack.key
```

For rpm packages, you have to import the key into the rpm key ring, using the following command:

```
# rpm --import bd-pack.key
```

If you want to check an rpm package, just issue a command similar to the following. You should get no error.

```
# rpm --checksig bitdefender-*.rpm
```

In case you are using the deb packages, you have to run only one command for all deb files.

```
# dpkg-sig --verify bitdefender-*.deb
```

4.2.3. Test FreeBSD tbz Package

When installing the package downloaded from the BitDefender servers, you should run **md5** on the package and compare the output with the value in the `.md5` file. This file is located in the same directory you downloaded the package from.

4.3. Install Product

There are two ways to install BitDefender Antivirus Scanner for Unices on your system:

- Using the self-extractable archive.
- Directly install the packages. As a general guideline, you have to first install the command line interface scanner and then the graphical user interface scanner.

4.3.1. Install with Self-extractable Archive

The self-extractable archive contains all the files required for installation. It acts as a shell script and it can be given several parameters in the command line. Usually, for a normal installation, no parameters are required: simply run the script.

Run Self-extractable Archive

To begin the installation, run the following command in the directory where the archive is located:

```
# sh BitDefender-Antivirus-Scanner-{ver}.{os}.{arch}.run
```

This will unpack the BitDefender files (engines, core, etc.), the install and uninstall scripts, and it will launch the installer, which, in turn, will install all BitDefender components, as described in the next section.

Installer

After unpacking the archive, the installer is launched. This is a text-based installer, created to run on very different configurations. Its purpose is to install the extracted packages at their locations and to configure BitDefender Antivirus Scanner for Unices for the first time, asking you just a few questions. To accept the default values the installer offers (which is recommended), just press the `ENTER` key.

First, the *License Agreement* is displayed. You are invited to read the full content by pressing the SPACE bar to advance one page or ENTER for one line a time. In order to continue the installation process, you must read and accept this License Agreement, by literally typing the word accept when prompted. Note that typing anything else or nothing at all means you do not agree with the License Agreement and the installation process will stop.

Once you have accepted the License Agreement terms, the installer will begin the installation process. Basically, it will install the engines, the binaries and the documentation and it will make the post-install configuration. This is a short list of its actions on your system.

- installs the manpages and configures the MANPATH accordingly
- creates a symbolic link to the bdscan command in /usr/bin/bdscan for Linux and /usr/local/bin/bdscan for FreeBSD
- configures the quarantine directory

After the command line interface scanner is installed, you will be prompted whether to install the graphical user interface scanner. If you do not want to install the GUI scanner, type N and then press the ENTER key. Otherwise, just press the ENTER key.

Additional Parameters

For the not-so-impatient user, the self-extractable archive supports a few command line parameters, described in the following table.

Parameter	Description
--help	Prints short help messages.
--info	Prints archive information, such as the title, the default target directory, the embedded script to be run after unpacking, the compression method used, the uncompressed size, the date of packaging.
--list	Prints the content of the embedded archive. The listed files are the engines, the program binaries, the embedded documentation, the install and uninstall script along with their size and permissions.
--check	This is one of the most useful options, because it enables the user to verify the package integrity, as stated above. The integrity is checked by comparing the embedded md5 checksum (generated during packaging) with the one computed at the time of the check. If they match, the output will be the following:

Parameter	Description

	`MD5 checksums are OK. All good.`
	If not, an error message will be shown, displaying the unmatching stored and computed checksums, such as:
	`Error in MD5 checksums:` *`X`* `is different from` *`Y`*

`--confirm`	The user will be asked to confirm every step of the install process.
`--keep`	By default, the archive content is extracted to a temporary directory, which will be removed after the embedded installer exits. Passing this parameter to the script will not remove the directory.
`--target` *`directory`*	You can specify another directory to extract the archive to, if you don't want to use the default name. Note that this target directory will not be removed.
`--uninstall`	Runs the embedded uninstaller script instead of the normal installer. To find out more about the uninstalling procedure, please refer to Chapter 5 "*Uninstall*" (p. 23).

4.3.2. Install rpm Packages

To install BitDefender Antivirus Scanner for Unices on a RedHat-based distribution using the RedHat package manager (**rpm**), follow these steps:

1. Install the command line interface scanner by running the following command in the directory the package is located in:

   ```
   # rpm -i bitdefender-scanner-{ver}.{os}.{arch}.rpm
   ```

2. If you want to use the graphical user interface scanner too, install it by running the following command in the directory where the package is located:

   ```
   # rpm -i bitdefender-scanner-gui-{ver}.{os}.{arch}.rpm
   ```

4.3.3. Install deb Packages

To install BitDefender Antivirus Scanner for Unices on a Debian-based distribution using the Debian package manager (**dpkg**), follow these steps:

1. Install the command line interface scanner by running the following command in the directory the package is located in:

   ```
   # dpkg -i bitdefender-scanner_{ver}.{os}.{arch}.deb
   ```

2. If you want to use the graphical user interface scanner too, install it by running the following command in the directory the package is located in:

   ```
   # dpkg -i bitdefender-scanner-gui_{ver}.{os}.{arch}.deb
   ```

4.3.4. Install ipk Packages

To install BitDefender Antivirus Scanner for Unices on Linux distributions that do not support **rpm** or **dpkg**, follow these steps:

1. Install the command line interface scanner by running the following command in the directory the package is located in:

   ```
   # /opt/ipkg/bin/ipkg-cl install \
   bitdefender-scanner_{ver}.{os}.{arch}.ipk
   ```

2. If you want to use the graphical user interface scanner too, install it by running the following command in the directory the package is located in:

   ```
   # /opt/ipkg/bin/ipkg-cl install \
   bitdefender-scanner-gui_{ver}.{os}.{arch}.ipk
   ```

4.3.5. Install FreeBSD Packages

To install BitDefender Antivirus Scanner for Unices on a FreeBSD system, follow these steps:

1. Install the command line interface scanner by running the following command in the directory the package is located in:

```
# pkg_add bitdefender-scanner-{ver}.tbz
```

2. **Only FreeBSD 6.x systems.** If you want to use the graphical user interface scanner too, install it by running the following command in the directory the package is located in:

```
# pkg_add bitdefender-scanner-gui-{ver}.tbz
```

5. Uninstall

There are two ways to remove BitDefender Antivirus Scanner for Unices from your system:

- Using the original self-extractable installation archive. This is the easiest and the recommended method.
- Directly uninstall the installed packages (`rpm`, `deb`, `ipk` or `tbz`). As a general guideline, you have to first uninstall the graphical user interface scanner and then the command line interface scanner.

5.1. Uninstall with Self-extractable Archive

The easiest way to completely remove BitDefender Antivirus Scanner for Unices, either from Linux or from FreeBSD systems, is to use the self-extractable archive. To proceed, you need the original self-extractable installation archive. This is necessary because the program will automatically undo all the settings used for integration with the system.

To begin the unistall process, run the following command in the directory the archive is located in:

```
# sh BitDefender-Antivirus-Scanner-{ver}.{os}.{arch}.run --uninstall
```

You must confirm your choice by pressing the `Y` and the `ENTER` keys.

First, the graphical user interface scanner is removed. Then, the command line interface scanner is removed. Finally, a message informs you when the uninstall process has been successfully completed. At that point, the system should be restored to the same condition it was in before the installation of BitDefender Antivirus Scanner for Unices.

5.2. Uninstall rpm Packages

To remove BitDefender Antivirus Scanner for Unices from a RedHat-based distribution using the RedHat package manager (**rpm**), follow these steps:

1. Remove the graphical user interface scanner (if installed) by running the following command:

```
# rpm -e bitdefender-scanner-gui
```

2. Remove the command line interface scanner by running the following command:

```
# rpm -e bitdefender-scanner
```

If you want to, you can remove only the graphical user interface scanner and continue to use the command line interface scanner.

5.3. Uninstall deb Packages

To remove BitDefender Antivirus Scanner for Unices from a Debian-based distribution using the Debian package manager (**dpkg**), follow these steps:

1. Remove the graphical user interface scanner (if installed) by running the following command:

```
# dpkg -r bitdefender-scanner-gui
```

2. Remove the command line interface scanner by running the following command:

```
# dpkg -r bitdefender-scanner
```

If you want to, you can remove only the graphical user interface scanner and continue to use the command line interface scanner.

5.4. Uninstall ipk Packages

To remove BitDefender Antivirus Scanner for Unices from Linux distributions that do not support **rpm** or **dpkg**, follow these steps:

1. Remove the graphical user interface scanner (if installed) by running the following command:

   ```
   # /opt/ipkg/bin/ipkg-cl remove bitdefender-scanner-gui
   ```

2. Remove the command line interface scanner by running the following command:

   ```
   # /opt/ipkg/bin/ipkg-cl remove bitdefender-scanner
   ```

If you want to, you can remove only the graphical user interface scanner and continue to use the command line interface scanner.

5.5. Uninstall FreeBSD (tbz) Packages

To remove BitDefender Antivirus Scanner for Unices from a FreeBSD system, follow these steps:

1. **Only FreeBSD 6.x systems.** Remove the graphical user interface scanner (if installed) by running the following command:

   ```
   # pkg_delete bitdefender-scanner-gui-{ver}
   ```

2. Remove the command line interface scanner by running the following command:

   ```
   # pkg_delete bitdefender-scanner-{ver}
   ```

On FreeBSD 6.x systems, you can also use **pkg_deinstall**, part of sysutils/portupgrade, as follows:

1. Remove the graphical user interface scanner (if installed) by running the following command:

   ```
   # pkg_deinstall bitdefender-scanner-gui
   ```

2. Remove the command line interface scanner by running the following command:

```
# pkg_deinstall bitdefender-scanner
```

Command Line Interface Scanner

6. Configuration File

The system-wide configuration of BitDefender Antivirus Scanner for Unices is stored inside a file located at `/etc/BitDefender-scanner/bdscan.conf` on Linux systems and at `/usr/local/etc/bitdefender-scanner/bdscan.conf` on FreeBSD systems. There is another configuration file, located inside the user's home directory, at `~/.config/BitDefender-scanner/bdscan.conf`, which is loaded after the system configuration. Therefore, the user can partially or even totally override the system settings.

System versus User configuration

This book covers the changes brought to the system-wide configuration file. Please remember that you can modify the current user's own configuration, with the same effect from his point of view.

The files are standard UNIX-style configuration files, based on `key=value` pairs, each pair on a single line.

A typical file on a Linux machine could be the following.

```
# An unpriviledged user can copy this file to
# ~/.config/BitDefender-scanner/bdscan.conf and change the settings
# to suit his/her needs. Any setting found in the home directory will
# overwrite the global one.
#
# Check the bdscan.conf(5) man page for more details.

# Where the product is installed
InstallPath = /opt/BitDefender-scanner

# In which directory should files be copied/moved if the action is
# "quarantine"
QuarantinePath = /opt/BitDefender-scanner/var/quarantine

# This file will be used by default for logging if the "--log"
# argument is used
LogName = /opt/BitDefender-scanner/var/log/bdscan.log

# By default bdscan scans all the files, but giving the "--ext"
# argument only files having the following extensions are scanned
Extensions = 386:asp:bas:bin:chm:cla:class:cmd:com:bat:csc:dat:dll:
doc:dot:exe:bat:hlp:hta:htm:html:ini:js:lnk:mdb:msi:nws:ocx:ole:
ovl:pfd:php:pif:pot:ppa:ppt:prc:rtf:scr:shs:smm:sys:url:vbe:vbs:
vxd:wbk:wdm:wiz:xla:xls:xlt:xml:xtp:

# The update location. Change this if you want to use an alternate
# update server.
UpdateHttpLocation = http://upgrade.bitdefender.com/update71

# If you use an HTTP proxy, uncomment the following line and specify
# the [[DOMAIN\]USERNAME[:PASSWRD]@]SERVER[:PORT] of the proxy
# server.
# e.g.: HttpProxy = myuser:mypassword@proxy.company.com:8080
#HttpProxy =

# Uncomment the following line after you insert your license key
#Key = enter_your_key_here
```

The available keys, their default values and description are presented in the table below. Some keys might not be present at a certain moment as their default values, defined internally, may need no change.

Key	Description
`InstallPath`	This is the path to the installation directory, which is set up during the installation process.
`UpdateHttpLocation`	The update location is the URL of the BitDefender update server, used when performing the triggered update. Default: `http://upgrade.bitdefender.com/update71`
`HttpProxy`	If a proxy server is required for Internet connection during updates, set this key accordingly. There is no default value. **More about triggered update** Please see Section *Triggered Update* (page 59) for more information about updates and proxy configuration.
`QuarantinePath`	This is the location of the quarantine directory where infected files are stored when quarantine actions are invoked.

Key	Description
	The quarantine directory can be specified at run-time using the `--quarantine=`*`path`* option. The default quarantine path is located at `/opt/BitDefender-scanner/var/quarantine`. **Regular Users and Quarantine** If the user does not have the right to put files into the quarantine directory, the program will exit with error and no scan will be performed. Therefore, you have to make sure you have the proper rights when using the quarantine action.
`LogName`	The log file contains all the output messages normally sent to `STDOUT`. The new log will be appended to the end of the last one at the following scan. If you want to clear the log file before scanning, you must use the `--log-overwrite` command line option. The log file can also be specified at run-time, using the `--log=`*`logfile`* option. The default log file is located at `/opt/BitDefender-scanner/var/log/bdscan.log`. If the user does not have the right to write it, the location becomes `~/.local/share/BitDefender-scanner/logs/bdscan.log`.
`Extensions`	The extensions list, with colon-separated items, specifies the file types to scan, identified by their extensions, when using the `--ext` command-line parameter. The list can be specified at run-time using the `--ext=`*`ext1`*`:`*`ext2`* option. To force the scanning of all files, regardless of the Extension directive, you must use the `--ext=:` form in the command line.
`ExcludeExtensions`	This list, with colon-separated items, specifies the file types to be excluded from scanning, identified by their extensions. The list can be specified at run-time using the `--exclude-ext=`*`ext1`*`:`*`ext2`* option.
`Key`	This is the license key, necessary for product activation.

Key	Description
	ℹ **Product Registration** Please refer to Chapter *Product Registration* (page 63) for more information about license keys.

7. Testing BitDefender

You can verify that BitDefender Antivirus Scanner for Unices works properly with the help of a special test file, known as the *EICAR Standard Anti-virus Test* file. EICAR stands for the *European Institute of Computer Anti-virus Research*. This is a dummy file, detected by antivirus products.

There is no reason to worry, because this file is not a real virus. All that `EICAR.COM` does when executed is to display the text `EICAR-STANDARD-ANTIVIRUS-TEST-FILE` and exit.

The reason we do not include the file in the package is that we want to avoid generating any false alarms for those who use BitDefender or any other virus scanner. However, the file can be created using any text editor, provided the file is saved in standard MS-DOS ASCII format and is 68 bytes long. It might also be 70 bytes if the editor adds CR/LF at the end. The file must contain the following single line:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Save the file under any name with the `.COM` extension, for example `EICAR.COM`. You can keep the `EICAR.COM` in a safe place and test the system protection periodically.

EICAR Online Resources

You can visit the EICAR website at http://eicar.com/, read the documentation and download the file from one of the locations on the web page http://eicar.com/anti_virus_test_file.htm.

7.1. Scan an Executable File

Open a new terminal and enter the directory the `EICAR.COM` file resides in. Type the following command:

```
# bdscan EICAR.COM
```

The output will indicate that one file has been scanned, found infected and that the virus was identified You will see the virus name: `EICAR-Test-File (not a virus)`. Since no action was specified, the file `EICAR.COM` is still on your hard disk.

The command output will be the following:

```
BitDefender Antivirus Scanner v7.60124 Linux-i686
Copyright (C) 1996-2008 BitDefender SRL. All rights reserved.
This program is licensed for commercial use.

Default action upon detecting an infected file: ignore action
Default action upon detecting a suspected file: ignore action
/tmp/EICAR.COM  infected: EICAR-Test-File (not a virus)


Results:
Folders           :0
Files             :1
Packed            :0
Archives          :0
Infected files    :1
Suspect files     :0
Warnings          :0
Identified viruses:1
I/O errors        :0
```

7.2. Scan an Archive

Next, you could archive or compress the file and run **bdscan** to scan inside the archive.

First, use the **gzip** command to create the compressed file. You can use several other tools, such as **zip**, **rar**, **arj** and so on.

```
# gzip -9  EICAR.COM
```

Then, use **bdscan** to scan this compressed file.

```
# bdscan  EICAR.COM.gz
```

BitDefender will unpack the archive and scan its content. This will be the command output:

```
BitDefender Antivirus Scanner v7.60124 Linux-i686
Copyright (C) 1996-2008 BitDefender SRL. All rights reserved.
```

```
This program is licensed for commercial use.

Default action upon detecting an infected file: ignore action
Default action upon detecting a suspected file: ignore action
/tmp/EICAR.COM.gz  ok
/tmp/EICAR ... >EICAR.COM  infected: EICAR-Test-File (not a virus)


Results:
Folders           :0
Files             :2
Packed            :0
Archives          :2
Infected files    :1
Suspect files     :0
Warnings          :0
Identified viruses:1
I/O errors        :0
```

7.3. Scan a Mailbox

BitDefender Antivirus Scanner for Unices can also unpack and scan mailboxes. If you wish to periodically scan your local mailbox, you can proceed as shown in the following example.

```
# bdscan mail.mbox
```

The e-mail messages in the mailbox will be read one by one, the attachments will be unpacked, their content will be extracted and, finally, scanned. BitDefender will display the subject of the infected e-mail, its date and the infected attachments.

```
BitDefender Antivirus Scanner v7.60124 Linux-i686
Copyright (C) 1996-2008 BitDefender SRL. All rights reserved.
This program is licensed for commercial use.

Default action upon detecting an infected file: ignore action
Default action upon detecting a suspected file: ignore action
/tmp/mail.mbox  ok
/tmp/mail.mbox=>(message 0)  ok
/tmp/mail.mbox=>(message 1)  ok
```

```
/tmp/mail.mbox=>(message 1)=> ... 34 +0300 (EEST)]=>(MIME part)  ok
/tmp/mail.mbox=>(message 1)=> ... =>(MIME part)=>(message body)  ok
/tmp/mail.mbox=>(message 1)=> ... 34 +0300 (EEST)]=>(MIME part)  ok
/tmp/mail.mbox=>(message 1)=> ... )]=>(MIME part)=>EICAR.COM.gz  ok
/tmp/mail. ... >EICAR.COM  infected: EICAR-Test-File (not a virus)
/tmp/mail.mbox=>(message 1)=> ... 34 +0300 (EEST)]=>(MIME part)  ok


Results:
Folders             :0
Files               :9
Packed              :0
Archives            :6
Infected files      :1
Suspect files       :0
Warnings            :0
Identified viruses:1
I/O errors          :0
```

8. Real Life Usage

These are some examples of real-life situations in which you can use BitDefender. Consider them to be guidelines on how to improve your system protection. If you have found a different way to use BitDefender Antivirus Scanner for Unices, do not hesitate to contact us and share your experience. You can write us at <documentation@bitdefender.com>.

8.1. Virus Scanning

BitDefender Antivirus Scanner for Unices is an excellent tool for the antivirus scanning of files and directories located in a filesystem. Here are some basic usage examples.

8.1.1. Scan a Regular File

If you just want to scan a simple file, you can run **bdscan** specifying the path to the file.

```
# bdscan --action=quarantine --verbose file.exe
```

As you can see below, one file was scanned and found infected, the virus was identified and it was moved to the quarantine directory. As verbose messages were requested, the name of the plugins used are also displayed.

You can use another action, such as `disinfect`, to try to disinfect the file first. Since not all files can be disinfected, you can try next to `quarantine` or even `delete` it.

Of course, you can use the `ignore` action (which is the equivalent of not specifying an action at all) and you will only be prompted when viruses are found. This behavior is extremely useful on read-only filesystems, such as optical disks (CD-ROM, DVD) or network filesystems mounted read-only.

```
BitDefender Antivirus Scanner v7.60124 Linux-i686
Copyright (C) 1996-2008 BitDefender SRL. All rights reserved.
This program is licensed for commercial use.
```

```
Default action upon detecting an infected file: ignore action
Default action upon detecting a suspected file: ignore action
/t ... xe  infected: EICAR-Test-File (not a virus) <- cevakrnl.xmd


Results:
Folders           :0
Files             :1
Packed            :0
Archives          :0
Infected files    :1
Suspect files     :0
Warnings          :0
Identified viruses:1
I/O errors        :0
```

8.1.2. Scan a Directory

The path to scan does not necessarily have to lead to a file; it can lead to any directory as well. BitDefender Antivirus Scanner for Unices can scan a directory tree, with unlimited recursion. You can adjust the recursion level by setting a fixed depth or by disabling recursion entirely.

Let's consider the following tree structure: one file and two sub-directories, each sub-directory containing several other files.

```
top_dir
|-- documents
|   |-- document1.doc
|   `-- document2.doc
|-- programs
|   |-- program1.exe
|   `-- program2.exe
`-- file.exe
```

If you to scan the `downloaded_files` directory, but not its sub-directories, the recursion level will be `1`. You might also want to quarantine the infected files, to study them later.

```
# bdscan --action=quarantine --recursive-level=1 top_dir
```

The screen output below shows the files scanned, found infected and finally quarantined. Please note that the two sub-directories were not scanned.

```
BitDefender Antivirus Scanner v7.60124 Linux-i686
Copyright (C) 1996-2008 BitDefender SRL. All rights reserved.
This program is licensed for commercial use.

Default action upon detecting an infected file: ignore action
Default action upon detecting a suspected file: ignore action
/tmp/top_dir/file.exe  infected: EICAR-Test-File (not a virus)
/tmp/top_d ... ument1.doc  infected: EICAR-Test-File (not a virus)
/tmp/top_d ... ument2.doc  infected: EICAR-Test-File (not a virus)
/tmp/top_d ... ogram1.exe  infected: EICAR-Test-File (not a virus)
/tmp/top_d ... ogram2.exe  infected: EICAR-Test-File (not a virus)


Results:
Folders           :3
Files             :5
Packed            :0
Archives          :0
Infected files    :5
Suspect files     :0
Warnings          :0
Identified viruses:1
I/O errors        :0
```

8.1.3. Scan Entire System

You might want to scan the entire system, not only some parts of it. Since **bdscan** does not scan symlinks, block and character devices, you can safely include `/dev` directory in your path.

The only problem is the number of target files and the time required to scan them, which could be very long, depending on your system's performance and filesystem capacity. By using a log file (which you will analyze at scan completion) you will reduce the screen output as only the infected and the suspected files will be dispalyed.

```
# bdscan --log=/tmp/bdscan.log --no-list /
```

Only the malware found will be displayed on the screen, but the log file will contain one line about every file scanned and its status. You can easily **grep** for “infected” and “suspected” keywords to see related report.

This is the beginning of the log file.

```
//
// BitDefender scan report
//
// Time: Fri Jan 27 15:24:03 2006
// Command line: --log=/tmp/bdscan.log --no-list /
// Core: AVCORE v1.0 (build 2266) (i386) (Mar  1 2005 19:34:16)
// Engines: scan: 13, unpack: 4, archive: 39, mail: 6
// Total signatures: 266776
//

/bin/dd ok
/bin/cp ok
/bin/df ok
/bin/ed ok
/bin/du ok
/bin/ln ok
/bin/ls ok
...
```

8.1.4. Scan Archives

BitDefender Antivirus Scanner for Unices can unpack and scan inside archives. There is a limit of archive recursion depth, to prevent the occurrence of exploits such as zip-bombs. You should be suspicious of any file archived recursively too many times.

Actions on Archives

Please note that some actions, such as `disinfect`, might fail when archives are scanned. This happens because BitDefender will not try or will not manage to recreate the archive after removing objects from it. Several closed-source compression algorithms are only free for uncompression and they require a valid license and registration for compression. Therefore, BitDefender can only unpack such an archive.

Let's suppose you have a many-times-archived file: `file.exe.tar.gz.bz2.zip.rar`. You can scan it, setting a maximum recursion level, by using this command:

```
# bdscan --verbose --archive-level=10 file.exe.tar.gz.bz2.zip.rar
```

As you can see, BitDefender reports to have scanned more files. This happens because each archive should be unpacked separately. You can also see which engine processes each unpacking and scanning step.

```
BitDefender Antivirus Scanner v7.60124 Linux-i686
Copyright (C) 1996-2008 BitDefender SRL. All rights reserved.
This program is licensed for commercial use.

Default action upon detecting an infected file: ignore action
Default action upon detecting a suspected file: ignore action
/tmp/file.exe.tar.gz.bz2.zip.rar  ok
/tmp/file.exe.tar.gz.bz ... file.exe.tar.gz.bz2.zip  ok <- rar.xmd
/tmp/file.exe.tar.gz.bz ... ip=>file.exe.tar.gz.bz2  ok <- zip.xmd
/tmp/file.exe.tar.gz.b ... tar.gz.bz2=>(bz2_data)  ok <- bzip2.xmd
/tmp/file.exe.tar.gz.bz ... bz2_data)=>file.exe.tar  ok <- gzip.xmd
/t ... xe  infected: EICAR-Test-File (not a virus) <- cevakrnl.xmd


Results:
Folders            :0
Files              :6
Packed             :1
Archives           :4
Infected files     :1
Suspect files      :0
Warnings           :0
Identified viruses:1
I/O errors         :0
```

8.1.5. Scan a Mailbox

If you want to scan your mailbox, or just some e-mail, messages, you can run BitDefender Antivirus Scanner for Unices on them. Each e-mail in the mailbox will be treated separately, its attachments extracted and scanned. The list of scanned objects can get very large, so you can use the logfile facility.

```
# bdscan --verbose mail.mbox
```

This example shows how an e-mail message containing a compressed attachment is scanned and the attached file is found to be infected.

```
BitDefender Antivirus Scanner v7.60124 Linux-i686
Copyright (C) 1996-2008 BitDefender SRL. All rights reserved.
This program is licensed for commercial use.

Default action upon detecting an infected file: ignore action
Default action upon detecting a suspected file: ignore action
/tmp/mail.mbox  ok
/tmp/mail.mbox=>(message 0)  ok <- mbox.xmd
/tmp/mail.mbox=>(message 1)  ok <- mbox.xmd
/tmp/mail.mbox=>(messag ... 00 (EEST)]=>(MIME part)  ok <- mime.xmd
/tmp/mail.mbox=>(messag ... E part)=>(message body)  ok <- mime.xmd
/tmp/mail.mbox=>(messag ... 00 (EEST)]=>(MIME part)  ok <- mime.xmd
/tmp/mail.mbox=>(messag ... IME part)=>EICAR.COM.gz  ok <- mime.xmd
/t ... OM  infected: EICAR-Test-File (not a virus) <- cevakrnl.xmd
/tmp/mail.mbox=>(messag ... 00 (EEST)]=>(MIME part)  ok <- mime.xmd


Results:
Folders           :0
Files             :9
Packed            :0
Archives          :6
Infected files    :1
Suspect files     :0
Warnings          :0
Identified viruses:1
I/O errors        :0
```

8.2. Report

You can request reports regarding the product's activity, status, known virus signatures or version.

8.2.1. Using Log File

You might want BitDefender to run in the background, with no user intervention, to display an enormous quantity of information or to keep its activity reports for later use. In these cases, you should use the log facility.

To specify a name for the log file, use the `--log=`*`logfile.log`* command line option. If the file already exists, it will be appended. You may use the `--log-overwrite` option to replace the old log file.

```
# bdscan --log=/tmp/antivirus_scan.log --log-overwrite file.exe
```

8.2.2. Get More Information

If you use the `--info` command line option, BitDefender will offer you information about its scanning engines, last update, key validity, etc.

```
# bdscan --info
```

Here is an example of what the screen output should read:

```
BitDefender Antivirus Scanner v7.60124 Linux-i686
Copyright (C) 1996-2008 BitDefender SRL. All rights reserved.
This program is licensed for commercial use.

Engine signatures: 266776
Scan engines: 13
Archive engines: 39
Unpack engines: 4
Mail engines: 6
System engines: 0
Update time GMT: Fri Jan 27 06:03:59 2006
Version: 7.05450
License expire date: Aug 26 2006
```

8.2.3. Display Virus List

BitDefender can print the virus list to standard output. Proceed with caution as the output will be heavy. To study the virus list, save it in a file on your local filesystem or send it to the pager, which will display it screen by screen.

```
# bdscan --virus-list | more
```

Using the pager's facilities, you can navigate inside the list or search for a virus name.

8.2.4. Display Product Version

If you need to find out the version of your installed BitDefender Antivirus Scanner for Unices, use the following command:

```
# bdscan --version
```

BitDefender will display the product's name, version and build number, architecture and copyright information.

```
BitDefender Antivirus Scanner v7.60124 Linux-i686
Copyright (C) 1996-2008 BitDefender SRL. All rights reserved.
```

8.3. Virus Submission

BitDefender will sometimes report *suspected* files. These are files that have not matched any virus signature, but which the heuristic analysis marked as possibly infected. They should be moved to the quarantine directory and submitted to BitDefender Antivirus Lab at <virus_submission@bitdefender.com> for further analysis.

Virus submission e-mails may be blocked by mail server antiviruses on their way to the BitDefender Antivirus Lab. Therefore, you should compress them in an encrypted zip archive and send both the archive and the password to it in the same e-mail.

To do this, you can use the command below:

```
# zip -e suspected.zip suspected_file
```

You will be prompted for a password twice. Pick out a simple password, as encryption is only used to scramble the file, not to protect it.

9. BitDefender Integration

BitDefender Antivirus Scanner for Unices is a versatile antivirus scanning solution, which can be integrated with desktop and e-mail server software to perform an instant target scan.

9.1. Desktop Integration

You can configure your favorite file manager, e-mail or news client to use BitDefender Antivirus Scanner for Unices for an instant file or e-mail scan. In some cases this is as simple as a mouse click, key-shortcut or menu selection.

These are only a few examples of how to run an antivirus scan on desktop applications.

9.1.1. Midnight Commander

> GNU Midnight Commander is a directory browser and file manager for Unix-like operating systems.
>
> —*The Midnight Commander manual page*

By pressing the **F2** key, you can easily access a user menu from which you can add extra features to the Midnight Commander. The menu can be edited by selecting **Command** → **Edit menu file**. You will be asked whether to edit the **Local** or the **Home** menu. Choose the **Home** menu so that changes are available in any directory.

The `menu` file will be opened in an editor. Go to the end of the file and append the lines below. Pay special attention to the blank spaces at the beginning of each line.

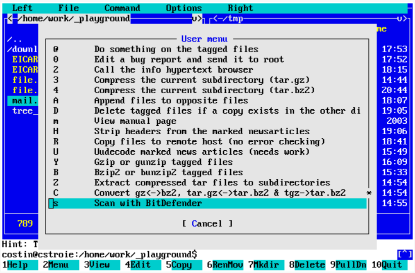
```
+ t rd & x /opt/BitDefender-scanner/bin/bdscan
s       Scan with BitDefender
        bdscan --no-list %s
        echo -n "Press ENTER to continue..."
        read
```

Different Installation Path

If you have used an installation path other than the default one, please change the first line accordingly. That condition ensures that the menu item is not shown if BitDefender Antivirus Scanner for Unices is not installed.

From now on, when you press the **F2** key on top of tagged or untagged files and directories, the User menu will pop-up and by pressing the **S** key you will scan the target against malware.

During the scan, you will not see the usual Midnight Commander interface, but the output screen. At the end, you have to press the `ENTER` key to return to the commander.



```
 Left     File     Command     Options     Right
<-/home/work/_playground--------v>  <-/tmp--------------------v>
                                                              me
/..        ---------------- User menu ----------------
/downl   @       Do something on the tagged files             17:53
 EICAR   0       Edit a bug report and send it to root        17:52
 EICAR   2       Call the info hypertext browser              18:15
 file.   3       Compress the current subdirectory (tar.gz)   14:44
 file.   4       Compress the current subdirectory (tar.bz2)  20:44
 mail.   A       Append files to opposite files               18:07
 tree_   D       Delete tagged files if a copy exists in the other di  19:05
         m       View manual page                              2003
         H       Strip headers from the marked newsarticles   19:06
         R       Copy files to remote host (no error checking)  18:41
         U       Uudecode marked news articles (needs work)   15:49
         Y       Gzip or gunzip tagged files                  16:09
         B       Bzip2 or bunzip2 tagged files                15:33
         Z       Extract compressed tar files to subdirectories  14:54
         C       Convert gz<->bz2, tar.gz<->tar.bz2 & tgz->tar.bz2  *  14:54
         s       Scan with BitDefender                        14:55

  789                        [ Cancel ]

Hint: T
costin@cstroie:/home/work/_playground$                          [^]
1Help  2Menu  3View  4Edit  5Copy  6RenMov 7Mkdir 8Delete 9PullDn 10Quit
```

Midnight Commander User Menu

9.1.2. KDE Konqueror

Konqueror is the file manager of K Desktop Environment. Using a specially crafted `.desktop` file, you can send any file or directory to BitDefender Antivirus Scanner for Unices for scanning. The output is displayed in a terminal emulator.

Copy the following file to `~/.kde/share/apps/konqueror/servicemenus/`, under the name `bitdefender.desktop`. You should also copy the `bitdefender.png` icon from the installation package to your icons directory.

Do not break the last line

The `Exec=...` line of this file has been broken for typographical reasons. When creating the file, remember to write it as a single line, as line breaking is not supported.

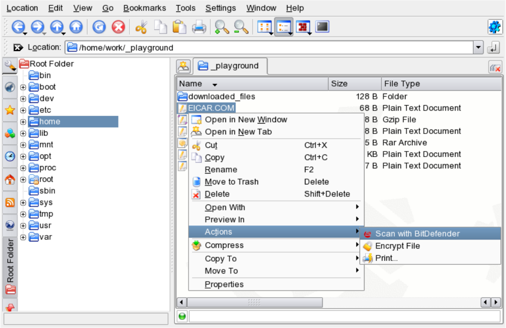
```
[Desktop Entry]
Name=BitDefender
Encoding=UTF-8
ServiceTypes=all/allfiles,inode/directory
TryExec=bdscan
Terminal=false
TerminalOptions=
Type=Application
Actions=Scan_With_BitDefender;
Icon=bitdefender

[Desktop Action Scan_With_BitDefender]
Name=Scan with BitDefender
Comment=Perform an AntiVirus scan with BitDefender
Icon=bitdefender
```

```
Exec=konsole -T "BitDefender Antivirus Scanner" --noclose \
     --nomenubar --notoolbar --icon bitdefender --vt_sz 80x25 \
     -e bdscan --no-list %f
```

You may now open **Konqueror**, right-click a file or directory and from the context menu select **Actions** → **Scan with BitDefender**.

A terminal window will open, displaying all the infected or suspected files found. At the end, a short summary will appear and the window will remain open until you close it.



Action on File in Konqueror

9.1.3. Krusader

> Krusader is an advanced twin panel (commander style) file manager for KDE, similar to Midnight or Total Commander (formerly Windows Commander), with many extras. It provides all the file-management features you could possibly want.
>
> —*Krusader home page*

When using Krusader, you can right-click a file or directory and select from the context menu **Konqueror menu** → **Actions** → **Scan with BitDefender**. This will work if you have followed the instructions in Section *KDE Konqueror* (page 46).

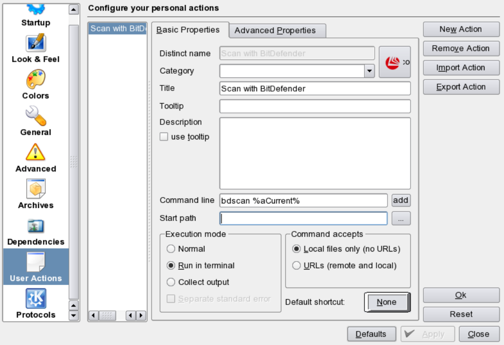
If not, Krusader offers its own way, called **Useractions**. You can add a new user action from the menu **Settings** → **Configure Krusader**; then, in the **User Actions** tab, press **New Action** and make the following changes:

- **Distinct name.** Set *Scan with BitDefender*.
- **Title.** Set *Scan with BitDefender*.
- **Tooltip.** Set *Perform an AntiVirus scan with BitDefender*.
- **Command line.** Set **bdscan --no-list %aCurrent%**.
- Then select the **Execution mode** → **Run in terminal** checkbox.

Press the **Ok** button and close the window.

A new item has appeared in the **Useractions** menu: **Scan with BitDefender**. Select it to start scanning the target files and directories.

The program output will be displayed in a console window, which will not close when the scanning process finishes. You will have to close it manually, after reading the messages.



Distinct name: Scan with BitDefender
Category:
Title: Scan with BitDefender
Tooltip:
Description:
☐ use tooltip
Command line: bdscan %aCurrent%
Start path:
Execution mode: ○ Normal ● Run in terminal ○ Collect output ☐ Separate standard error
Command accepts: ● Local files only (no URLs) ○ URLs (remote and local)
Default shortcut: None

Krusader User Actions

9.1.4. ROX-Filer

> ROX is a fast, user friendly desktop which makes extensive use of drag-and-drop. The interface revolves around the file manager, or filer, following the traditional Unix view that 'everything is a file' rather than trying to hide the filesystem beneath start menus, wizards, or druids.
>
> —*ROX-Wiki*

ROX-Filer provides a **SendTo** context menu, to open the selected file with the desired program. In this case, the program will be a shell script, wrapping BitDefender and displaying its output in a terminal window.

Copy the following shell script, name it `BitDefender` and save it in the `~/.rox_choices/SendTo/` directory.

```
#!/bin/sh
# BitDefender ROX-Filer integration script
# Copyright (C) 1996-2008 BitDefender SRL. All rights reserved.

# Place this script in your home directory, at the next location:
# ~/.rox_choices/SendTo

# Now let's run the scan process
xterm -e "bdscan --no-list $*; \
          echo -n 'Press ENTER to continue...'; \
          read"

# End of the script
```

Do not forget to give it executable rights.

```
# chmod 755 ~/.rox_choices/SendTo/BitDefender
```

You can right-click a file or a directory, select **Send to** → **BitDefender** menu and the scanning process will start. When the scan is finished, you will need to close the window, after reading the output messages.

9.1.5. Pine

> Pine® - a Program for Internet News & Email - is a tool for reading, sending, and managing electronic messages.
>
> —*Pine Information Center*

To scan an e-mail from a mail user agent, you have to save the message in the filesystem and scan that file. Fortunately, these actions can be done automatically, by using a shell script. Save the following file to a convenient location, such as the BitDefender installation directory, `/opt/BitDefender-scanner`. Name it `bdscanpipe` and remember the full path to it: `/opt/BitDefender-scanner/bin/bdscanpipe`.

```
#!/bin/sh
# BitDefender STDIN scanner integration script
# Copyright (C) 1996-2008 BitDefender SRL. All rights reserved.

# Place this script in your BitDefender installation directory
# and name it bdscanpipe, such as:
#   /opt/BitDefender-scanner/bin/bdscanpipe

# Set some parameters
BDSCAN=bdscan
TMPFILE=/tmp/bdscanpipe_$$

# Save the standard-input to a temporary file
cat > $TMPFILE

# Scan it with BitDefender and remember the exitcode
$BDSCAN $TMPFILE
```

```
EXIT=$?

# Remove the temporary file and return the exitcode
rm -f $TMPFILE
exit $EXIT

# End of the script
```

Action on Infected E-mail

You will not be able to disinfect a message which BitDefender has found to be infected. The only action that can be taken is `ignore`. Therefore you can choose whether to delete or move the e-mail or, even better, instruct the e-mail client to do so.

If you want to be able to scan e-mail messages from Pine using BitDefender, you have to change your Pine settings to enable Unix pipe commands. To do so, follow these steps.

Start Pine and type **S** (for Setup), then **C** (for Config). Use the down-arrow key to find and highlight **enable-unix-pipe-cmd** (somewhere under Advanced Command Preferences) and enable this preference by typing **X**. Type **E** (for Exit Setup) and **Y** when asked to Save Changes.

Now, in the Index screen and when displaying the e-mail, there is one more command: **| Pipe**, ready to be tested.

1. When an e-mail message is displayed or in the Index screen, press the **| Pipe** key (**Shift**+****).
2. The entire message must be sent to the filter, so press **Control**+**W** (Raw text). The status line should display the message: `Pipe RAW message X to :`.
3. Type the full path to the filter, not only the script name. For example: `/opt/BitDefender-scanner/bin/bdscanpipe`. Press **ENTER**.

This is what the screen should read:

```
Pipe RAW message 299 to : /opt/BitDefender-scanner/bin/bdscanpipe
^G Help                 ^W Shown Text  ^R With Delimiter
^C Cancel  Ret Accept ^Y Free Output
```

The full e-mail will be piped to the BitDefender filter, which will temporarily save it on the filesystem and scan the resulting file with **bdscan**. After the scan, the output results will be displayed by Pine and they will indicate whether the e-mail was infected or not. When you have finished reading the messages, press**E** to Exit the viewer.

As stated before, it would be better to request that Pine automatically scan the messages and instruct it what to do when an infected e-mail message is found. In this way, every new message will be scanned and treated accordingly, which will reduce their displaying speed.

Possible actions to be taken on infected e-mail:

- Set a keyword (e.g. `Infected`) and add an IndexColor rule to highlight the message tagged with this keyword.
- Move the e-mail to a safe location, to study it carefully.
- Remove the e-mail.

Creating Filter Rules

You can create a filter rule to move the infected e-mail to another mailbox. Follow these steps:

1. Type **S** (for Setup), then **R** (for Rules) and **F** (for Filters). Then press **A** (Add) to add a new rule.

2. Name the rule (e.g. *BitDefender Antivirus Scan*).

3. Select **Current Folder Type** → **Email** to apply the rule to all e-mail folders. You can also select **Message is New (Unseen)?** → **Yes**, to only scan new e-mail messages, therefore increasing the overall scanning speed.

4. Scroll down to **External Categorizer Commands** and set the following values:
   - **Command**: `/opt/BitDefender-scanner/bin/bdscanpipe`
   - **Exit Status Interval**: `(1,254)`

5. Scroll down to **Filter Action** and select **Move**. You must specify the folder the infected e-mail is to be moved to.

6. Finally, select **Set New Status** → **Clear this state** and **Features** → **dont-stop-even-if-rule-matches**. Type **E** (for Exit) and **Y** when asked to Save Changes.

From now on, when a new e-mail message is received, it will be piped to the BitDefender filter and, if found infected, it will be moved to a safe location.

9.1.6. Evolution

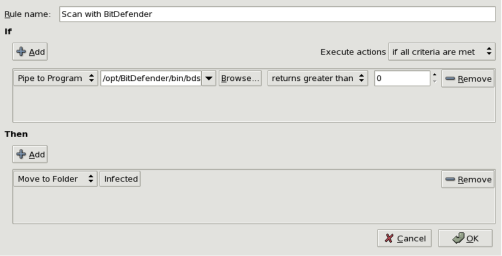
> Evolution makes the tasks of storing, organizing, and retrieving your personal information easy, so you can work and communicate more effectively with others. It's a highly evolved groupware program, an integral part of the Internet-connected desktop.
>
> —*Evolution User Guide*

You can set Evolution to scan e-mail messages with BitDefender by using e-mail Filters. In this way, any newly downloaded message will be sent to scanning.

BitDefender pipe: bdscanpipe

Evolution needs a filter to pipe messages into. Please review Section *Pine* (page 49) and use the provided script.

First, add a new filter rule: **Tools** → **Filters...**, then press **Add**. Name the rule *Scan with BitDefender* and add to the **If** panel the rule **Pipe to Program**. Fill in the program name, `/opt/BitDefender-scanner/bin/bdscanpipe`, and set the condition **returns greater than** and value `0`.


Rule name: Scan with BitDefender

If

Execute actions: if all criteria are met

Pipe to Program | /opt/BitDefender/bin/bds | returns greater than | 0

Then

Move to Folder | Infected

Evolution Filter Configuration

Next, in the **Then** panel, you will set the action to be taken on infected e-mail. For example, you can move it to a special folder (named *Infected*), set a color code to mark it or just delete it.

Once the filter is configured, any new e-mail will be piped into the scanning filter. If you want to scan only some e-mail messages, add corresponding rules to the **If** panel.
To manually scan a highlighted message, press **Control**+**Y** keys.

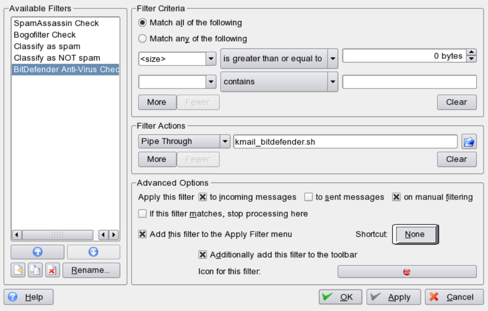
9.1.7. KMail

> KMail is a fully-featured e-mail client that fits nicely into the K Desktop Environment, KDE. It has features such as support for IMAP, POP3, multiple accounts, powerful filters, PGP/GnuPG privacy, inline attachments, and much more.
>
> —*KMail website*

To integrate BitDefender with KMail, use the wizard in the **Tools** → **Anti-virus Wizard...** menu. This will autodetect BitDefender and will automatically configure the filters to pipe any message. A script will add an `X-Virus-Flag` header to the message, with values `Yes` or `No`, depending on whether the e-mail is infected or not.

If you do not want to use the wizard, you can manually add the filter rule. Follow these steps:

1. Go to **Settings** → **Configure filters...**.
2. Add a new filter and name it *BitDefender Anti-Virus Check*.
3. In the **Filter Criteria** panel, add a rule to select which messages to scan, for example a rule that will scan all messages.



Available Filters

- SpamAssassin Check
- Bogofilter Check
- Classify as spam
- Classify as NOT spam
- BitDefender Anti-Virus Chec

Filter Criteria

● Match all of the following

○ Match any of the following

<size>	is greater than or equal to	0 bytes
	contains	

Filter Actions

Pipe Through	kmail_bitdefender.sh

Advanced Options

Apply this filter ☒ to incoming messages □ to sent messages ☒ on manual filtering

□ If this filter matches, stop processing here

☒ Add this filter to the Apply Filter menu Shortcut: None

☒ Additionally add this filter to the toolbar

Icon for this filter:

KMail Filter Configuration

4. In the **Filter Actions** panel, select **Pipe Through** and type `kmail_bitdefender.sh` in the textbox.
5. Select the **Apply to incoming message** and **Apply on manual filtering** check boxes.
6. Press the **OK** button to save the new rule.

Copy the following script, name it `kmail_bitdefender.sh` and save it somewhere in your path.

```
#!/bin/sh
# BitDefender KMail integration script
# Copyright (C) 1996-2008 BitDefender SRL. All rights reserved.
# Place this script in your PATH and name it
# kmail_bitdefender.sh, such as: ~/bin/kmail_bitdefender.sh

# Set some parameters
BDSCAN=bdscan
TMPFILE=/tmp/bdkmail_$$

# Save the standard-input to a temporay file
cat > $TMPFILE

# Scan it with BitDefender, filter the output and echo the header
if $BDSCAN $TMPFILE | grep -q infected; then
  echo "X-Virus-Flag: yes"
else
  echo "X-Virus-Flag: no"
fi

# Output the email and remove the temporary file
cat $TMPFILE
rm $TMPFILE

# End of the script
```

You can even customize this filter yourself. You can add a convenient button on the toolbar to call the filter on a highlighted message

Filter Actions in KMail

Due to the current KMail structure, the script is called in the **Actions** section on the filter. This means that the only action the filter can take is add a header indicating whether the message is infected or not. It is up to you to add another filter to check for this header and to perform any desired action

9.2. Mail Server Integration

BitDefender Antivirus Scanner for Unices can also be used to scan the e-mail traffic passing through an e-mail server. Additional tools enable you to integrate the server and the antivirus. These are just a few examples of how to make a low-budget e-mail scanner using BitDefender Antivirus Scanner for Unices.

9.2.1. Qmail-Scanner

> Qmail-Scanner is an add-on that enables a Qmail e-mail server to scan all gateway-ed e-mail for certain characteristics (i.e. a content scanner).
>
> —*Qmail-Scanner website*

Qmail-Scanner supports BitDefender Antivirus Scanner for Unices out of package. To use it, you can just proceed to normal installation, since the configuration script will automatically detect BitDefender. Alternately, you can pass options to the script, such as specifying the antivirus to use.

Qmail-Scanner Installation

Qmail-Scanner supports many installation options, for fine-grained qmail integration. Please refer to the documentation for further instructions.

Enter the directory where you have unpacked the Qmail-Scanner archive, and run the following command:

```
# ./configure --scanners bitdefender
```

Once configuration is done, you can install Qmail-Scanner by running the following command:

```
# ./configure --install
```

Having done this, you can start testing Qmail-Scanner by sending test e-mail messages to a local account. You should watch the logs for possible errors.

9.2.2. MailScanner

> A Free Anti-Virus and Anti-Spam Filter.
>
> —*MailScanner website*

Integrating MailScanner with BitDefender is a very simple process. Since BitDefender Antivirus Scanner for Unices is supported by MailScanner by default, all you need to do correctly install MailScanner and to modify one line.

MailScanner Installation

Please refer to the on-line or printed MailScanner documentation for details on its installation.

Once you have a working MailScanner installed on your server, open its configuration file `/opt/MailScanner/etc/MailScanner.conf` (for a default location) and find the line below:

```
Virus Scanners = none
```

Change it as follows:

```
Virus Scanners = bitdefender
```

If you need to further customize the command-line options passed to BitDefender, open file `/opt/MailScanner/lib/bitdefender-wrapper` and change the corresponding line, located at the end of the file.

9.2.3. amavisd-new

> amavisd-new is a high-performance interface between mailer (MTA) and content checkers: virus scanners, and/or SpamAssassin.
>
> —*amavisd-new website*

amavisd-new supports BitDefender for e-mail scanning by default. All you have to do is make sure to install all the prerequisites (mainly additional perl modules), then install amavisd-new according to the instructions in its documentation.

Before using it in real situations, it would be better for you to check that BitDefender was properly detected. Therefore, run the command below and watch for the line indicating that bdscan has been found.

```
# amavisd-new debug
```

The output will also contain this line:

```
Found primary av scanner BitDefender at /usr/bin/bdscan
```

This is all you have to do. You can test mail server integration using EICAR e-mail messages.

amavisd-new Installation

Please refer to the amavisd-new documentation for a detailed description of its installation and configuration.

10. Updates

BitDefender Antivirus Scanner for Unices was designed with triggered update capabilities. Nowadays, the risk of getting infected is high, both because new viruses appear and because the existing ones keep spreading. This is why your antivirus must be kept up to date. To do so, you must periodically check the BitDefender servers for new updates.

10.1. Triggered Update

10.1.1. Run Triggered Update

BitDefender Antivirus Scanner for Unices is configured to update automatically, when triggered by the following command:

```
# bdscan --update
```

The output should be the following:

```
BitDefender Antivirus Scanner v7.60124 Linux-i686
Copyright (C) 1996-2008 BitDefender SRL. All rights reserved.
This program is licensed for commercial use.

/opt/BitDefender-scanner/var/lib/scan/Plugins/emalware.ivd ........
...................................................... updated
/opt/BitDefender/var/lib/scan/Plugins/update.txt  updated
Update succeeded.
```

10.1.2. Regular Updates

If you want **bdscan** to get the latest virus definitions and signatures on a regular basis, you can use the cron service, which is installed by default on most Linux distributions.

Edit Cron Table

The first update method is to edit the **cron** tables, using the **crontab** tool. For example, if you want to set a daily update, run the following as root:

```
# crontab -e
```

Then add this line:

```
00 02 * * * /opt/BitDefender-scanner/bin/bdscan --update
```

All you have to do now is to signal the **cron** daemon to reload the crontables. Run the command below and look for the process-id of **crond**, located in the second column.

```
# ps aux  | grep crond
```

With the process-id (*`PID`*) in mind, issue the following command to signal the **crond** daemon. Replace *`PID`* with the corresponding process-id value.

```
# kill -HUP PID
```

In this way, you will run the update at 2:00 AM.

Use cron.* Scheduling Facility

Depending on your Linux distribution, you can use another regular update method. Most major distributions use **cron** to run scripts located in several directories, on a hourly, daily, weekly and monthly basis. Although not very accurate, this method provides a very simple way to add a new job to or to remove it from **cron**.

First, you should look for several directories, such as `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly` and `/etc/cron.monthly`. For this example you could use the `cron.daily` or even `cron.hourly` directories.

Create the a file as shown below, name it `bdscan-update` and place it in the selected directory. Do not forget to change the `INSTALL_PATH`, if you have not used the default installation location.

```
#!/bin/sh
# BitDefender update script, using cron service
# Copyright (C) 1996-2008 BitDefender SRL. All rights reserved.

# Place this script under one of the following directories for daily
# or even hourly updates (find their equivalents on your system if
# they do not exactly match):
# /etc/cron.daily
# /etc/cron.hourly

# IMPORTANT: change this parameter according to your installation
BDSCAN=/opt/BitDefender-scanner/bin/bdscan

# Now let's run the update process
$BDSCAN --update

# End of the update script
```

Finally, make the script executable using this command.

```
# chmod 755 bdscan-update
```

You can even try to manually run the script, to test whether it works properly.

10.1.3. HTTP Proxy

If you are using an HTTP proxy server to connect to the Internet, the triggered update may fail because the BitDefender update server cannot be reached.

To specify a proxy server to be used when updating, you must open the configuration file, usually located at `/etc/BitDefender-scanner/bdscan.conf`, and add the line below. You should replace the sample values according to your conditions.

```
HttpProxy = your.proxy.server:port
```

10.2. Manual Update

If you have no Internet access so that **bdscan** cannot check and download updates, you can perform a manual update. The update server hosts a `cumulative.zip` archive, released every day, containing all of the scanning engines and virus signatures updates up to the release date. You can use this archive to update BitDefender.

Let BDPATH be the path to the BitDefender Antivirus Scanner for Unices installation directory. For Linux systems BDPATH is /opt/BitDefender-scanner, while for FreeBSD systems BDPATH is /usr/local/bitdefender-scanner. To update the product manually, follow these steps:

1. **Download the update files.** Download the cumulative.zip file from one of the following locations and save it somewhere on your disk when prompted.
   - For 32-bit systems: http://download.bitdefender.com/updates/update_av32bit/
   - For 64-bit systems: http://download.bitdefender.com/updates/update_av64bit/
2. **Extract the updates.** Extract the content of the zip archive to the $BDPATH/var/lib/scan/ directory, overwriting the existing files with the newer ones, if necessary.
3. **Set file owner and permissions.** After extracting the zip archive, you **must** set the proper owner and permissions, by running the following commands:

```
# chown root:root $BDPATH/var/lib/scan/Plugins/*
# chmod 644 $BDPATH/var/lib/scan/Plugins/*
```

11. Product Registration

The product is delivered with a trial registration key valid for thirty days. At the end of the trial period, if you want to continue using the program, you have to provide a new license key.

When you have the new key, open the configuration file in `/etc/BitDefender-scanner/bdscan.conf` (for a default Linux installation) or in `/usr/local/etc/bitdefender-scanner/bdscan.conf` on FreeBSD systems and find the line similar to this one:

```
Key =  00112233445566778899
```

Simply replace the old key value with the new one and save the file.

Check Expire Date

If you want to check the key expiration date, please run the command below and read its output.

```
# bdscan --info
```

11.1. Trial License

By default, the product comes with a trial key which allows it to be used in any way or environment whatsoever for 30 days from the install time. When the trial period expires, all of the product features regarding scan actions (disinfect, delete) will be disabled and the user will have to either go online to www.bitdefender.com and register for a personal license or purchase a commercial license from the nearest BitDefender dealer.

11.2. License for Home or Personal Use

This is a free license, which you can retrieve from the BitDefender website after filling in a short form. It allows you to use the product only for personal purposes, with no commercial implications whatsoever. For example, the Personal License, allows you to scan your personal laptop or desktop computer but NOT TO USE IT IN A PRODUCTION ENVIRONMENT, SUCH AS AN OFFICE COMPUTER OR A COMPANY SERVER.

11.3. License for Commercial Use

If you plan on using BitDefender Antivirus Scanner for Unices with your own integration system or pre-designed scripts, you must purchase the Commercial License. The commercial license allows unlimited and unrestricted usage of the product in any environment whatsoever. The Commercial License is sold per user, depending on how many users benefit from the product's features.

12. Best Practices

These are a few guidelines on how to make sure your system is free from viruses.

1. After installing BitDefender Antivirus Scanner for Unices, perform a triggered update to get the latest virus signatures and engines, as described in Section *Triggered Update* (page 59).
2. Perform a full system scan to find any already infected objects. Use the guidelines in Chapter *Real Life Usage* (page 37).
3. Make sure the license key has not expired and get a new one before the expiring date. Read more about license keys in Chapter *Product Registration* (page 63).
4. If you are using **cron** or another method to do regular updates, make sure the job scheduler really works and that you always get the latest updates.
5. When using the `quarantine` action, which moves infected objects to the quarantine directory, keep an eye on it. Periodically check the directory size, since it can grow rapidly and you could run out of disk space. Take a look at the files BitDefender has found infected. You could simply remove them if you are sure they are infected, you can double check them (the suspected objects can be false positive alarms) and you can send them to BitDefender Antivirus Lab, as described below, for in-depth analysis.
6. Use BitDefender Antivirus Scanner for Unices to scan all the files you have from untrusted sources, such as the Internet, web browsing or the e-mail. Scan the documents, archives, programs and anything else that could contain malicious code. Periodically perform a full system scan.
7. Send all suspected objects to BitDefender Antivirus Lab, at <`virus_submission@bitdefender.com`>, for a prompt response to malware threats. To prevent this kind of e-mail from being filtered by an antivirus protecting e-mail servers, you should archive the suspected object, encrypt the archive and send them both, together with the key.

13. Frequently Asked Questions

1. Installation

1. What are the system requirements?

   Check Section 3.1 “*System Requirements*” (p. 9).

2. Does BitDefender alter my system configuration?

   Yes, for manpage integration, BitDefender Antivirus Scanner for Unices will alter several system files (`man.config` and `manpath.config`), if they are found on the system. It will also create certain symlinks in the `/etc` and `/usr/bin` directories for Linux and in `/usr/local/etc` and `/usr/local/bin` directories for FreeBSD.

2. Usage

1. My **bdscan** program has found a virus in a file, but it does not disinfect it, although I know it can be done. Why does it not disinfect the file?

   The `--action` command line option, whose default value is `ignore`, can be used to specify the action to be applied when a virus is found. Other possible values are `disinfect`, `delete`, `quarantine` or `ignore`.

   Please note that there are a lot of malicious applications, included in the *malware* category, which cannot be disinfected because of their internal structure and behavior. Therefore, if **bdscan** finds such a piece of malware, it is recommended that you delete the file infected with it.

2. How can I tell the virus signatures database is up to date?

   Run the following command and look for the line indicating the time of the last update:

   ```
   # bdscan --info
   ```

If your BitDefender Antivirus Scanner for Unices performs a regular updates, the latest one should be quite recent. If not, this is a good moment for you to update your antivirus.

3. When I try to update the virus definitions/scanning engines, I always get this message: “No update available”. Why?

Make sure you are not running the update as an unprivileged user, (i.e. not `root`), because, if this is the case, you do not have the right to write in the Plugins directory. This is normal and secure behavior.

Another possibility would be that there really are no updates available at that time, which may happen if you run updates very often.

4. How often are updates released and how can I always get the latest updates? How do I know when updates are released?

New updates are released as soon as new malwares is identified, which happens every few hours. BitDefender Antivirus Scanner for Unices can be configured to check for updates every few hours, using the **cron** daemon.

5. When I try move infected or suspected files to the quarantine zone, I get a “move failed” message in the log file. Why?

Make sure you have the proper rights with respect to the quarantine directories, i.e. the directories must be writable by those who want to use the quarantine facility. The default install creates the quarantine directories with `rwx` access rights for all users. If you are an admin of the Linux system, and you use the quarantine facility, make sure to check those directories from time to time, and delete all unnecessary files, to free up disk space.

6. Why doesn't **bdscan** scan symbolic links?

bdscan does not follow symbolic links by default, in order to prevent unauthorized disk access and recursive loops, especially for the `/dev` and `/proc` directories. However, if you are sure you want to scan symlinks, you can use the `--follow-link` option.

Manual Pages

bdscan

bdscan — BitDefender Antivirus Scanner for Unices

Synopsis

`bdscan` [--action= disinfect | quarantine | delete | ignore] [--no-archive] [--no-mail] [--no-pack] [--no-recursive] [--follow-link] [--recursive-level=*level*] [--archive-level=*level*] [--ext[=*ext1:ext2*]] [--exclude-ext[=*ext1:ext2*]] [--suspect-copy] [--suspect-move] [--quarantine=*quarantine_path*] [--conf-file=*conf_file*] [--log[=*file.log*]] [--log-overwrite] [--no-list] [--no-warnings] [--verbose] [--update] [--force-insecure-update] [--virus-list] [--info] [--version] [--encode=password] [--help] `path-to-scan`

Description

bdscan is the console of the BitDefender virus scanner for Unices. It may come as a standalone package, as well as integrated in the BitDefender mail or file server antivirus suite.

BitDefender Antivirus Scanner for Unices is mainly used scan files against any kind of viruses, trojans, worms or other malware. It uses the most advanced scanning engine technology to provide high rates of detection, reliability and speed.

The user can choose to move to quarantine directories, disinfect or delete the infected and suspected files. **bdscan** also has the capacity to scan inside mailboxes for infected attachments.

Options

`path-to-scan`
: The path to scan can be a list of files and directories, separated by white spaces.

`--action`
: Specifies the action to be performed when an infected object is found. See the **Actions** section for action details.

`--no-archive`
: Specifies that **bdscan** should not scan inside archives.

`--no-mail`
Specifies that **bdscan** should not scan inside mailboxes.

`--no-pack`
Specifies that **bdscan** should not scan inside packed programs.

`--no-recursive`
Specifies that **bdscan** should not enter sub-directories for scanning. If you select this option only the first level directories will be scanned.

`--follow-link`
Instructs **bdscan** to scan symbolic links.

`--recursive-level=`*`level`*
Sets the maximum recursion level to *`level`*. The default value is `0`, meaning no limitation.

`--archive-level=`*`level`*
Set the maximum archive depth level to *`level`*. The default value is `12`.

`--ext[=`*`ext1:ext2`*`]`
Specifies that **bdscan** should only scan files the extensions of which are specified in the list or in the configuration file, under the `Extensions` keyword. To force the scanning of all files, regardless of the Extension directive, you must use the `--ext=:` from in the command line.

`--exclude-ext[=`*`ext1:ext2`*`]`
Specifies that **bdscan** should exclude from scanning the files the extensions of which are specified in the list. If the list is empty, the extensions from the configuration files are to be used.

`--suspect-copy`
Specifies that **bdscan** should copy the suspected files to quarantine.

`--suspect-move`
Specifies that **bdscan** should move the suspected files to quarantine.

`--quarantine=`*`path`*
Sets the quarantine directory, where infected files are stored when the action is `quarantine`. If the user cannot write into the quarantine directory, bdscan will exit with error when the quarantine action is invoked.

`--conf-file=`*`file`*

Sets the alternate location of the configuration file. If this file is not valid, bdscan will exit with an error message. By default, the configuration is read from `/etc/BitDefender-scanner/bdscan.conf` on Linux systems and from `/usr/local/etc/bitdefender-scanner/bdscan.conf` on FreeBSD systems. There is also a local configuration file located at `~/.config/BitDefender-scanner/bdscan.conf`, the user being able to partially or even totally override the system-wide configuration.

`--log[=`*`file.log`*`]`

Specifies that **bdscan** should log its activity to the mentioned file. If the user has no right to write this file, the output will be an error message and the default file will be used. The default file is `/opt/BitDefender-scanner/var/log/bdscan.log`.

`--log-overwrite`

Specifies that **bdscan** should not append the new output to the existing log file. The old log file content will be replaced by the new one.

`--no-list`

Specifies that **bdscan** should not list all the scanned files. This option can speed up the scanning process.

`--no-warnings`

Specifies that **bdscan** should not display warnings. Warnings are displayed in case part of a virus signature has been found.

`--verbose`

Specifies that **bdscan** should output detailed messages.

`--update`

Specifies that **bdscan** should automatically update the virus signatures.

`--force-insecure-update`

Instructs **bdscan** to download updates without verifying the server signature file. This option is not recommended, but may be useful if regular update fails.

`--virus-list`

Displays the virus list. This could cause a lot of information to be displayed.

`--info`

Prints information about the products version, current number of virus signatures, last update time, scan engine number, archive engines, unpack engines, mail engines and system engines.

`--version`

Displays a short message containing the version information and the copyright note.

`--encode=`*`password`*

Encrypts the `password` you provide. You can use this option to encrypt the proxy user password and then copy the hash in the configuration file.

`--help`

Displays the help message.

Actions

When an infected object is found, **bdscan** can be instructed to perform one of the following actions:

`disinfect`

BitDefender will try to disinfect the object by removing the infected or suspected part. The action can sometimes fail.

`quarantine`

The object will be moved from its original location to a secured directory, the quarantine.

`delete`

The object will be simply removed from the filesystem

`ignore`

Even if infected objects are found, BitDefender will just report them and no action will be performed. This is the default action.

Examples

```
# bdscan --no-archive --verbose --action=disinfect /var/tmp
```

In the command line above, **bdscan** is instructed to scan the `/var/tmp` directory, archives excluded, display detailed messages and try to disinfect the files.

```
# bdscan  --no-mail  --log=/tmp/bdscan.log  --action=quarantine  /var/tmp
```

In the command line above, **bdscan** is instructed to scan the `/var/tmp` directory, mailboxes excluded, log its activity into the `/tmp/bdscan.log` file and quarantine the infected files.

Files

`/etc/BitDefender-scanner/bdscan.conf`
: The system-wide configuration file of **bdscan** on Linux systems. The user configuration overrides the system-wide configuration.

`/usr/local/etc/bitdefender-scanner/bdscan.conf`
: The system-wide configuration file of **bdscan** on FreeBSD systems. The user configuration overrides the system-wide configuration.

`~/.config/BitDefender-scanner/bdscan.conf`
: The user configuration file of **bdscan**. The user configuration overrides the system-wide configuration.

Bugs

Sometimes, **bdscan** may hang while scanning directories which contain pipes or UNIX socket files. To avoid this behavior, try to use it on regular files exclusively.

Although highly unlikely, **bdscan** may crash while scanning files. If this is the case, you should update the scan engines and the virus signatures and definitions.

See also

Please also refer to the printed and on-line BitDefender documentation at http://www.bitdefender.com.

Graphical User Interface Scanner

14. Getting Started

After installing BitDefender Antivirus Scanner for Unices, you can start using it. To do this, use one of these methods:

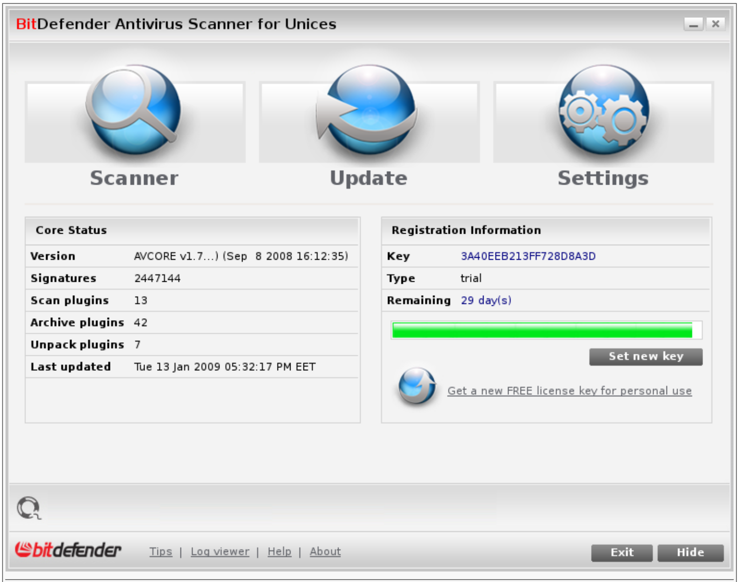
- Open a terminal and run the following command:

  ```
  # bdgui
  ```

  Note
  You can run this command both as a root and as a regular user.

- On Gnome desktops, follow this path: **Applications** → **System Tools** → **BitDefender Scanner**.
- On KDE desktops, follow this path: **Applications** → **System** → **BitDefender Scanner**.
- On Xfce desktops, either click the Xfce menu or right-click the desktop, and then follow this path: **System** → **BitDefender Scanner**.

The main interface is displayed.



BitDefender Antivirus Scanner for Unices

Core Status

Version	AVCORE v1.7...) (Sep 8 2008 16:12:35)
Signatures	2447144
Scan plugins	13
Archive plugins	42
Unpack plugins	7
Last updated	Tue 13 Jan 2009 05:32:17 PM EET

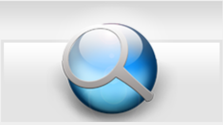
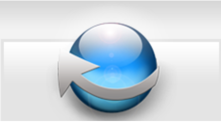
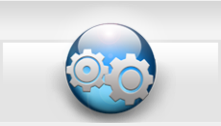
Registration Information

Key	3A40EEB213FF728D8A3D
Type	trial
Remaining	29 day(s)

Set new key
Get a new FREE license key for personal use
bitdefender
Tips | Log viewer | Help | About
Exit
Hide

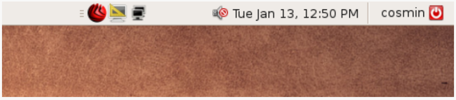
BitDefender GUI

Three buttons are available in the upper part of the window:

Button	Description
	**Scanner**. Click it to start scanning your computer for viruses and other malware.
	**Update**. Click it to update BitDefender, thus keeping the malware signatures database up to date.
	**Settings**. Click it to customize your BitDefender.

To close the window, click the **Exit** button.

If you configure BitDefender to run in the background, a **Hide** button is available next to **Exit**. Click this button to hide the window. You can restore it by clicking the BitDefender icon in the system tray.



BitDefender Icon in System Tray

If you right-click this icon, the following options are available:

Show/Hide
Display/Hide the main interface.

Exit
Exit the application.

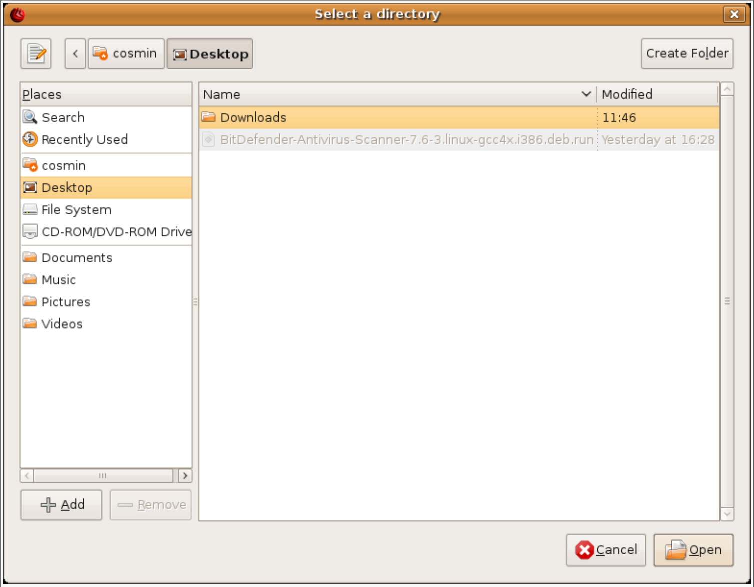
14.1. Scanning with BitDefender

There are several ways to set BitDefender to scan the files and folders on your computer:

- Drag&drop the file or directory you want to scan on the main window.
- Click the **Scanner** button, select the file or directory you want to scan and click **Open**.
- If you have configured BitDefender to run in the background, you can use the file drop zone. For more information, please refer to Chapter 16 "*File Drop Zone*" (p. 97).

To scan your computer for viruses and other malware, follow these steps:

1. Click the Scanner button. A new window will appear.

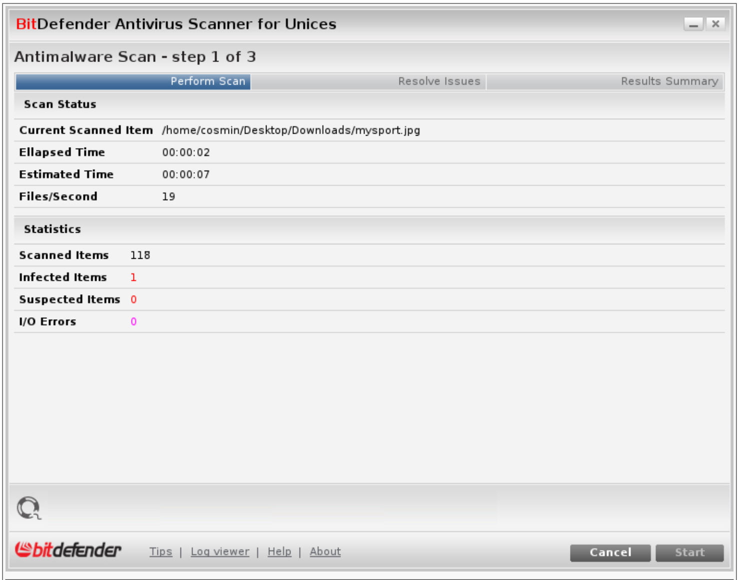


Name	Modified
Downloads	11:46
BitDefender-Antivirus-Scanner-7.6-3.linux-gcc4x.i386.deb.run	Yesterday at 16:28

Choose location

2. Choose the location (file or folder) to be scanned and click **Open**.

3. BitDefender will start scanning the selected objects. Wait for BitDefender to finish scanning.


BitDefender Antivirus Scanner for Unices

Antimalware Scan - step 1 of 3

Scan Status

Current Scanned Item	/home/cosmin/Desktop/Downloads/mysport.jpg
Ellapsed Time	00:00:02
Estimated Time	00:00:07
Files/Second	19

Statistics

Scanned Items	118
Infected Items	1
Suspected Items	0
I/O Errors	0

Scanning

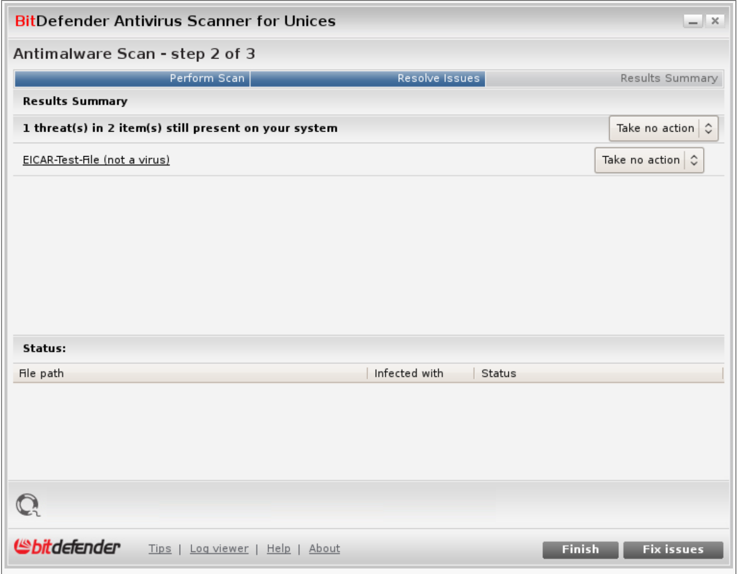
You can see the scanning location, status and statistics (scanning speed, elapsed time, number of scanned / infected / suspicious / hidden objects and other).

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

You can stop scanning anytime you want by clicking **Cancel**. You will go directly to the last step of the wizard.

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

Note
You will skip this step if no threats are found.



BitDefender Antivirus Scanner for Unices

Antimalware Scan - step 2 of 3

Results Summary

1 threat(s) in 2 item(s) still present on your system — Take no action

EICAR-Test-File (not a virus) — Take no action

Status:

File path	Infected with	Status

Actions

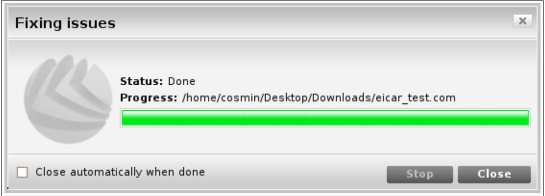
You can see the number of issues affecting your system. To find out more information about a specific threat detected on your system, just click it.

You can choose an overall action to be taken for all issues or you can select separate actions for each group of issues.

The following options can appear on the menu:

Action	Description
Take No Action	No action will be taken on infected files.
Disinfect	Removes the malware code from the infected files.
Delete	Removes the infected files from the disk.
Quarantine	Moves the infected files from their original location to the quarantine folder.

Click **Fix issues** to apply the specified actions.



Fixing issues

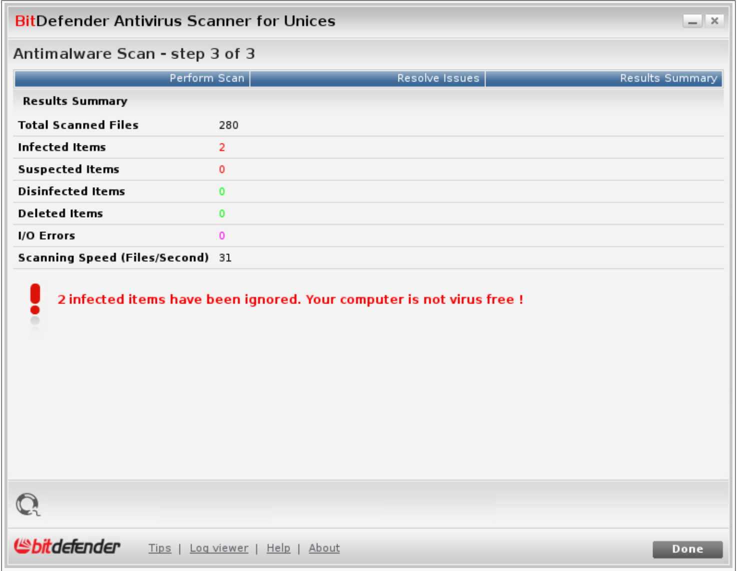
Status: Done

Progress: /home/cosmin/Desktop/Downloads/eicar_test.com

□ Close automatically when done

Fix issues

5. When BitDefender has finished fixing the issues, click **Close** and then **Finish**. The scan results will appear in a new window.



BitDefender Antivirus Scanner for Unices

Antimalware Scan - step 3 of 3

Results Summary

Total Scanned Files	280
Infected Items	2
Suspected Items	0
Disinfected Items	0
Deleted Items	0
I/O Errors	0
Scanning Speed (Files/Second)	31

2 infected items have been ignored. Your computer is not virus free !

Summary

You can see the results summary.

Click **Done** to close the window.

14.2. Updating BitDefender

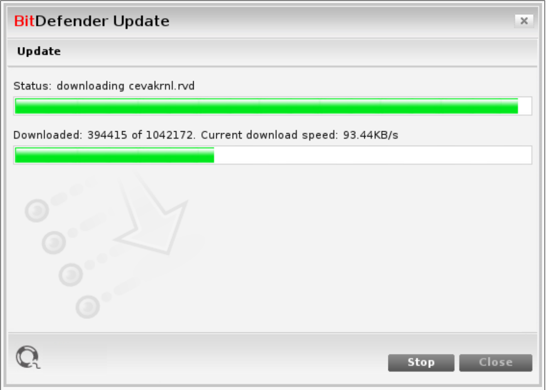
New malware is found and identified every day. This is why it is very important to keep BitDefender up to date with the latest malware signatures.

Note
As a best practice, you should update BitDefender before scanning files or folders from your computer.

The update of the malware signatures is only performed on demand. The update process is very simple, quick and effective.

To update BitDefender, follow these steps:

1. Click the Update button. A new window will appear.



Status: downloading cevakrnl.rvd

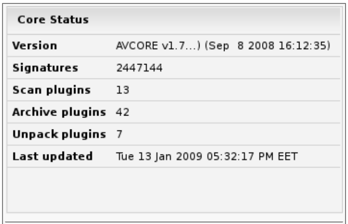
Downloaded: 394415 of 1042172. Current download speed: 93.44KB/s

Updating BitDefender

2. Wait for the update to complete.
3. Click **Close**.

In the Core Status area, you can find out relevant information about the antivirus engine and the updates, namely:

- antivirus engine version
- number of virus signatures
- number of scan plugins
- number of archive plugins
- number of unpack plugins
- last update



Core Status

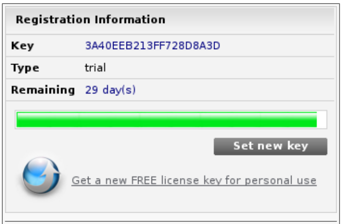
Version	AVCORE v1.7...) (Sep 8 2008 16:12:35)
Signatures	2447144
Scan plugins	13
Archive plugins	42
Unpack plugins	7
Last updated	Tue 13 Jan 2009 05:32:17 PM EET

Core Status

14.3. Registering BitDefender

The Registration Information area provides relevant information regarding the registration status, as follows:

- current license key
- license key type
- remaining validity period



Registration Information

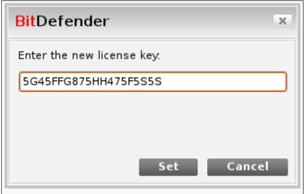
Key	3A40EEB213FF728D8A3D
Type	trial
Remaining	29 day(s)

Registration Information

If you are using a trial version, or if the product is about to expire or has already expired, a **Get a new FREE license key for personal use** link will also be available. Click this link to obtain a license key for free from the BitDefender website. You will have to fill in a form in order to receive your free license key.

To register BitDefender Antivirus Scanner for Unices:

1. Click the **Set new key** button. A new window will appear.



Enter the new license key:

5G45FFG875HH475F5S5S

Add new key

2. Type the new license key into the corresponding field.
3. Click **Set**.

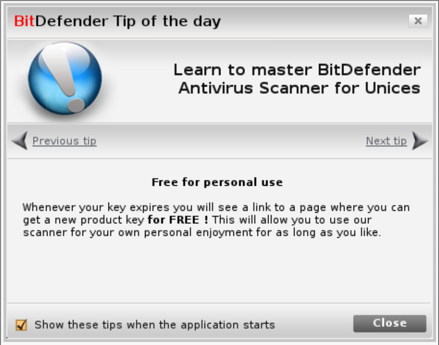
14.4. Finding Additional Information

Several links are available in the bottom area of the BitDefender interface. These links help you find out additional information on BitDefender.

Link	Description
Tips	Click it to open the tips window.
Log viewer	Click it to view the scan logs.
Help	Click it to open the help file.
About	Click it to find out more information about BitDefender Antivirus Scanner for Unices.

14.4.1. Tips

Whenever you start BitDefender, a tips window is displayed on top of the main interface.


BitDefender Tip of the day
Learn to master BitDefender Antivirus Scanner for Unices
Previous tip
Next tip

Free for personal use

Whenever your key expires you will see a link to a page where you can get a new product key **for FREE !** This will allow you to use our scanner for your own personal enjoyment for as long as you like.

☑ Show these tips when the application starts
Close

Tips Window

Tips provide useful information on how to use BitDefender. Use the corresponding links to go to the next tip or to return to the previous tip.

If you no longer want to see the tips when you start BitDefender, clear the **Show these tips when application starts** check box. Click the **Close** button to close the window.

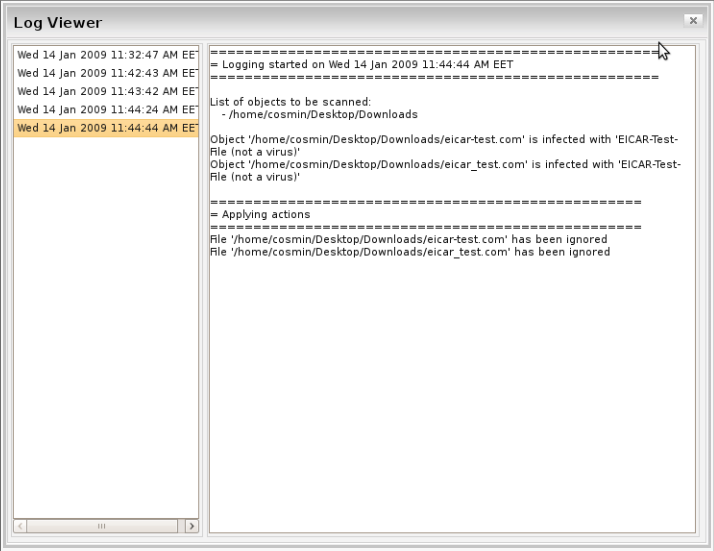
You can open the tips window at any time by clicking the **Tips** link.

14.4.2. Log Viewer

By default, BitDefender creates a log file for every scan. The log file contains valuable information regarding the scan process, such as the scan path and the infected files detected.

Note
The default directory where logs are saved is: `$HOME/.local/share/BitDefender-scanner/logs`

To view a scan log, open the Log Viewer by clicking the **Log Viewer** link.


Log Viewer
Wed 14 Jan 2009 11:32:47 AM EET
Wed 14 Jan 2009 11:42:43 AM EET
Wed 14 Jan 2009 11:43:42 AM EET
Wed 14 Jan 2009 11:44:24 AM EET
Wed 14 Jan 2009 11:44:44 AM EET

```
===========================================================
= Logging started on Wed 14 Jan 2009 11:44:44 AM EET
===========================================================

List of objects to be scanned:
   - /home/cosmin/Desktop/Downloads

Object '/home/cosmin/Desktop/Downloads/eicar-test.com' is infected with 'EICAR-Test-
File (not a virus)'
Object '/home/cosmin/Desktop/Downloads/eicar_test.com' is infected with 'EICAR-Test-
File (not a virus)'

==========================================================
= Applying actions
==========================================================
File '/home/cosmin/Desktop/Downloads/eicar-test.com' has been ignored
File '/home/cosmin/Desktop/Downloads/eicar_test.com' has been ignored
```

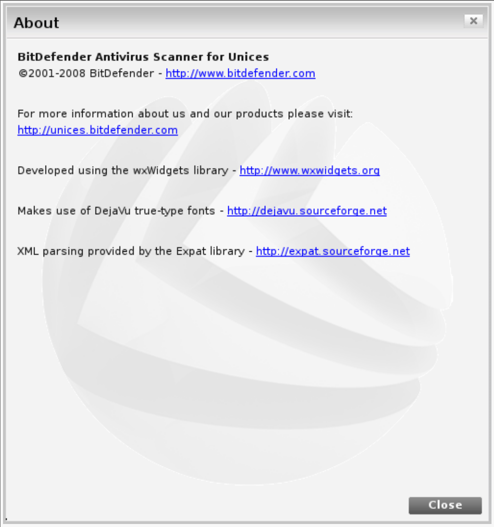
Log Viewer

Select the scan log from the left side menu to view information about the respective scan process.

In time, the number of logs displayed in the Log Viewer will increase, making it difficult to browse logs. To clear the Log Viewer, you must delete the logs directory manually, from the command line. The directory will be automatically created the next time you scan your computer.

14.4.3. About BitDefender

To find out more information about BitDefender Antivirus Scanner for Unices, click the **About** link. An information window will appear.



BitDefender Antivirus Scanner for Unices
©2001-2008 BitDefender - http://www.bitdefender.com

For more information about us and our products please visit:
http://unices.bitdefender.com

Developed using the wxWidgets library - http://www.wxwidgets.org

Makes use of DejaVu true-type fonts - http://dejavu.sourceforge.net

XML parsing provided by the Expat library - http://expat.sourceforge.net

About

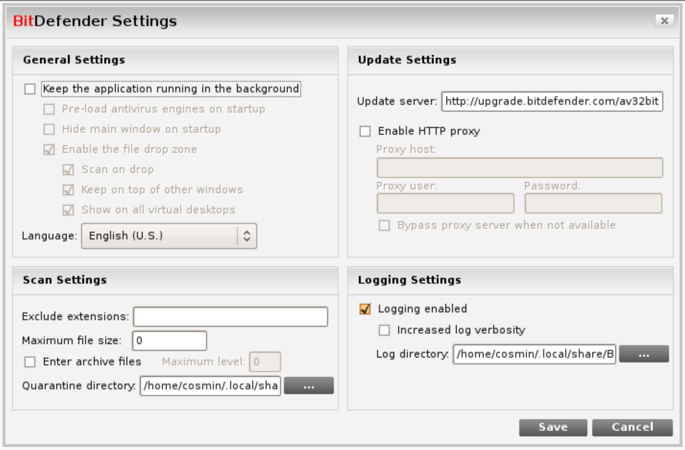
Click the **Close** button to close the window.

15. Configuring BitDefender

You can easily customize your BitDefender Antivirus Scanner for Unices according to your scanning needs.

- In order to be able to start scanning tasks quickly, you can pre-load the antivirus engines at startup..
- The duration of the scanning process can be dramatically reduced by excluding special files from scanning.
- A specific location can be set both for the quarantined files and for the log files.
- If your computer is connected to the Internet through a proxy server, you can configure the proxy settings.

To access these settings and customize your BitDefender Antivirus Scanner for Unices, click the Settings button. A new window will appear.



General Settings

☐ Keep the application running in the background
☐ Pre-load antivirus engines on startup
☐ Hide main window on startup
☑ Enable the file drop zone
☑ Scan on drop
☑ Keep on top of other windows
☑ Show on all virtual desktops
Language: English (U.S.)

Update Settings

Update server: http://upgrade.bitdefender.com/av32bit
☐ Enable HTTP proxy
Proxy host:
Proxy user:
Password:
☐ Bypass proxy server when not available

Scan Settings

Exclude extensions:
Maximum file size: 0
☐ Enter archive files Maximum level: 0
Quarantine directory: /home/cosmin/.local/sha

Logging Settings

☑ Logging enabled
☐ Increased log verbosity
Log directory: /home/cosmin/.local/share/B

Configuring BitDefender

The settings are organized into four areas:

- General Settings
- Scan Settings
- Update Settings
- Logging Settings

Change the settings according to your needs and click the **Save** button to save the changes and close the window.

15.1. General Settings

In this area, the following settings are available:

Keep the application running in the background

By selecting this check box, BitDefender will run in the background and act as a scan server for future instances. In this case, the antivirus engines will no longer be loaded for each scan request (which speeds up the scanning process), but the system memory usage will be higher.

Pre-load antivirus engines on startup

By selecting this check box, the antivirus engines will be loaded the first time the application runs. This speeds up the scanning process at the cost of greater application load times and a higher memory footprint.

When the option is disabled (default), the engines are loaded every time you initiate a scan request.

Hide main window on startup

By selecting this check box, the main window will be hidden automatically when you start your computer. You can use the BitDefender icon in the system tray to restore the window at a later time.

Warning

If your window manager or desktop environment does not provide a system tray, you should not enable this option.

Enable the file drop zone

By selecting this check box, a large BitDefender icon (the file drop zone) is displayed on your desktop. You can drag&drop files or folders on this icon to quickly scan them.

Scan on drop

Select this check box to immediately start scanning any file or directory dropped on the file drop zone.

If you disable this option, the file drop zone acts as a “scan queue” to which you can add files and directories from multiple sources. You can then scan all the items in the queue by simply double-clicking the file drop zone.

Keep on top of other windows

Select this check box so that the file drop zone is always displayed on top of other windows.

Show on all virtual desktops

Select this check box so that the file drop zone is displayed on all of your virtual desktops.

Language

You can use this menu to change the language of the BitDefender interface.

Note

You must restart the application for this setting to take effect.

15.2. Scan Settings

In this area, the following settings are available:

Exclude extensions

This is where you can list the file extensions to be excluded from scanning. Use `:` to separate them.

Maximum file size

This is where you can set the maximum size of the files to be scanned. Files exceeding this limit will not be scanned. To scan all files, regardless of their size, set the limit to `0`.

Note

Valid measurement unit specifiers are: `b` or `B` for bytes, `k` or `K` for kilobytes (1 KB = 1024 B), `m` or `M` for megabytes (1MB = 1024 KB), `g` or `G` for gigabytes (1 GB = 1024 MB). Example: `1m512k` specifies a maximum size of `1.512 MB`.

Warning
It is considered an error to specify more than `1023` of a given sub-unit. For example, `1024k` is invalid because `1024` kilobytes is equal to `1` megabyte (the correct form is `1m`). Setting an incorrect value here will cause the application to silently ignore this setting.

Enter archive files

By selecting this check box, archived files will be scanned. This provides increased detection at the cost of higher system resource usage during scanning.

Maximum level

This is where you can specify the maximum recursion level when processing archives inside archives. To scan all archives, regardless of the recursion level, set the limit to `0`. Higher values provide increased detection at the cost of higher system resource usage during scanning.

Quarantine directory

This is where you can specify a fully-qualified path to a directory where infected files will be moved when the **Quarantine** option is selected. The directory will be created if it does not already exist.

Note
The default quarantine directory is:
`$HOME/.local/share/BitDefender-scanner/quarantine`

15.3. Update Settings

In this area, the following settings are available:

Update server

This is where you can set the server to be queried for updated malware signatures.

Enable HTTP proxy

Select this check box if you use an HTTP proxy server when downloading antivirus updates. You must configure the proxy settings as follows:

Proxy host

Type the host name or the IP address of the proxy server and the port used to connect to the proxy server. They must be specified as follows: `host[:port]`.

Proxy user

Type a user name recognized by the proxy server. The user name must be specified as follows: `[domain\]username`.

Leave the field blank if the proxy server does not require authentication.

Password

Type the password of the specified user.

Leave the field blank if the proxy server does not require authentication.

Bypass proxy server when not available

Select this check box for a direct connection to be used if the proxy server is not available.

15.4. Logging Settings

In this area, the following settings are available:

Logging enabled

By selecting this check box, BitDefender will create and manage detailed log files recording the actions it performs.

Increased log verbosity

By selecting this check box, extra information is recorded in the log files. This includes logging every file scanned, every file that is excluded from scanning due to specific scan settings, etc.

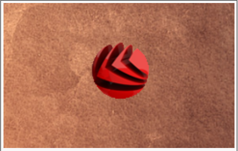
Log directory

This is where you can specify a fully-qualified path to a directory where log files will be stored. The directory will be created if it does not already exist.

Note

The default directory where logs are saved is: `$HOME/.local/share/BitDefender-scanner/logs`

16. File Drop Zone



File Drop Zone

If you configure BitDefender to run in the background, you can choose to enable the file drop zone. The file drop zone is a large BitDefender icon, displayed on your desktop, on which you can drag&drop files and directories to be scanned. In this way, you can easily scan files and directories, without having to open the main interface.

You can move and place this icon wherever you want on your desktop.

16.1. Enabling File Drop Zone

The file drop zone is not enabled by default. To enable it, follow these steps:

1. Open the main interface.
2. Click the **Settings** button.
3. Select the **Keep the application running in the background** check box.
4. Select the **Enable the file drop zone** check box.

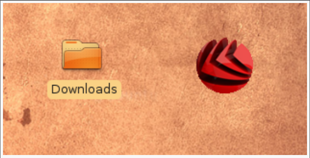
16.2. Scanning Files and Directories

The file drop zone helps you easily scan files and directories. You can choose between two scan types:

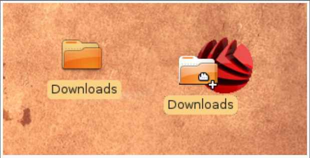
- **Immediate scanning** - an object is scanned as soon as you drop it on the file drop zone. This is the default setting.
- **Queued scanning** - you drag&drop the objects to be scanned on the file drop zone and then manually start the scan.

16.2.1. Immediate Scanning

By default, BitDefender immediately scans any object that you drop on the file drop zone. The following images illustrate the drag&drop procedure:



Drag Object



Drop Object

You must follow the Antimalware Scan wizard to complete the scan.

16.2.2. Queued Scanning

Queued scanning allows scanning files and directories from multiple sources at a time.

To switch from immediate scanning to queued scanning, follow these steps:

1. Open the main interface.
2. Click the **Settings** button.
3. Clear the **Scan on drop** check box.

When queued scanning is in use, you can notice a number in the center of the file drop zone. This number indicates how many objects are in the scan queue.

To perform queued scanning, follow these steps:

1. Drag&drop the files and directories you want to scan on the file drop zone.
2. Start scanning manually by doing either of the following:

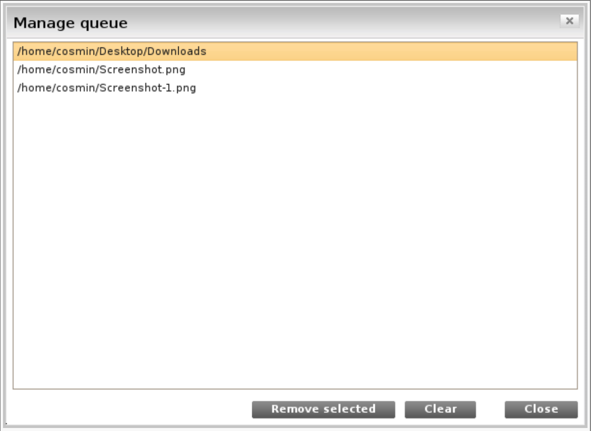
- Double-click the file drop zone.
- Right-click the file drop zone and select **Start scanning**.

3. Follow the Antimalware Scan wizard.

Managing Queued Items

If you want to quickly reset the queue, right-click the file drop zone and select **Clear queue**.

To review and manage the objects in the scan queue, right-click the file drop zone and then click **Manage queued items**. A new window will appear.


Manage queue
/home/cosmin/Desktop/Downloads
/home/cosmin/Screenshot.png
/home/cosmin/Screenshot-1.png
Remove selected
Clear
Close

Manage Queue

To remove specific objects from the queue, select them and click **Remove selected**. If you want to remove all objects from the queue, just click **Clear**.

Click the **Close** button to close the window.

Getting Help

17. Support

BitDefender strives to provide its customers with an unparalleled level of fast and accurate support. If you experience any issue with or if you have any question about your BitDefender product, go to our online Support Center. It provides several resources that you can use to quickly find a solution or an answer. Or, if you prefer, you can contact the BitDefender Customer Care team. Our support representatives will answer your questions in a timely manner and they will provide you with the assistance you need.

17.1. BitDefender Support Center

BitDefender Support Center, available at http://www.bitdefender.com/businesshelp, is the place where you will find all the assistance you need with your BitDefender product.

You can use several resources to quickly find a solution or an answer:

- Knowledge Base Articles
- BitDefender Support Forum
- Product Documentation

You can also use your favorite search engine to find out more information about computer security, the BitDefender products and the company.

Knowledge Base Articles

The BitDefender Knowledge Base is an online repository of information about the BitDefender products. It stores, in an easily accessible format, reports on the results of the ongoing technical support and bugfixing activities of the BitDefender support and development teams, along with more general articles about virus prevention, the management of BitDefender solutions with detailed explanations, and many other articles.

The BitDefender Knowledge Base is open to the public and freely searchable. The extensive information it contains is yet another means of providing BitDefender customers with the technical knowledge and insight they need. All valid requests for information or bug reports coming from BitDefender clients eventually find their way into the BitDefender Knowledge Base, as bugfix reports, workaround cheatsheets or informational articles to supplement product helpfiles.

The BitDefender Knowledge Base for business products is available any time at http://www.bitdefender.com/businesshelp.

BitDefender Support Forum

The BitDefender Support Forum provides BitDefender users with an easy way to get help and to help others. You can post any problem or question related to your BitDefender product.

BitDefender support technicians monitor the forum for new posts in order to assist you. You may also get an answer or a solution from a more experienced BitDefender user.

Before posting your problem or question, please search the forum for a similar or related topic.

The BitDefender Support Forum is available at http://forum.bitdefender.com, in 5 different languages: English, German, French, Spanish and Romanian. Click the **Business Protection** link to access the section dedicated to business products.

Product Documentation

Product documentation is the most complete source of information about your product.

You can check and download the latest version of documentation for BitDefender business products at Support Center > Documentation.

17.2. Asking for Assistance

To contact us for assistance:

1. Go to http://enterprise.bitdefender.com/support/contact-us.html.
2. Use the contact form to open an email support ticket or access other available contact options.

17.3. Contact Information

Efficient communication is the key to a successful business. During the past 10 years BITDEFENDER has established an unquestionable reputation by constantly striving for better communication so as to exceed the expectations of our clients and partners. Should you have any questions, do not hesitate to contact us.

17.3.1. Web Addresses

Sales Department: <sales@bitdefender.com>
Support Center: http://www.bitdefender.com/businesshelp
Documentation: <documentation@bitdefender.com>
Local Distributors: http://www.bitdefender.com/partners
Partner Program: <partners@bitdefender.com>
Media Relations: <pr@bitdefender.com>
Job Opportunities: <jobs@bitdefender.com>
Virus Submissions: <virus_submission@bitdefender.com>
Spam Submissions: <spam_submission@bitdefender.com>
Report Abuse: <abuse@bitdefender.com>
Web site: http://www.bitdefender.com

17.3.2. BitDefender Offices

The BitDefender offices are ready to respond to any inquiries regarding their areas of operation, both in commercial and in general matters. Their respective addresses and contacts are listed below.

United States

BitDefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
United States
Phone (sales&technical support): 1-954-776-6262
Sales: <sales@bitdefender.com>
Web: http://www.bitdefender.com
Support Center: http://www.bitdefender.com/businesshelp

Germany

BitDefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Phone (office&sales): +49 (0)2301 91 84 222
Phone (technical support): +49 (0)2301 91 84 444
Sales: <vertrieb@bitdefender.de>
Website: http://www.bitdefender.de
Support Center: http://www.bitdefender.de/businesshelp

UK and Ireland

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
UK
Phone (sales&technical support): +44 (0) 8451-305096
Email: <info@bitdefender.co.uk>
Sales: <sales@bitdefender.co.uk>
Website: http://www.bitdefender.co.uk
Support Center: http://www.bitdefender.co.uk/businesshelp

Spain

BitDefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
España
Fax: (+34) 93 217 91 28
Phone (office&sales): (+34) 93 218 96 15
Phone (technical support): (+34) 93 502 69 10
Sales: <comercial@bitdefender.es>
Website: http://www.bitdefender.es
Support Center: http://www.bitdefender.es/businesshelp

Romania

BITDEFENDER SRL

West Gate Park, Building H2, 24 Preciziei Street
Bucharest, Sector 6
Fax: +40 21 2641799
Phone (sales&technical support): +40 21 2063470
Sales: <sales@bitdefender.ro>
Website: http://www.bitdefender.ro
Support Center: http://www.bitdefender.ro/businesshelp

United Arab Emirates

Bitdefender FZ-LLC
Dubai Internet City, Building 17
Office # 160
Dubai, UAE
Phone (sales&technical support): 00971-4-4588935 / 00971-4-4589186
Fax: 00971-4-44565047
Sales: <sales@bitdefender.com>
Web: http://www.bitdefender.com/world
Support Center: http://www.bitdefender.com/businesshelp

Glossary

ActiveX

ActiveX is a model for writing programs so that other programs and the operating system can call them. The 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.

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 scanning method 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 scanning method 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 communication channel between two computers.

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.

Script

Another term for macro or batch file, a script is a list of commands that can be executed without user interaction.

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.

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 computer communication standards and conventions for network connections and traffic routing.

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, update installation routines 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.

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.