bitdefender ®

antivirus

Antivirus scanner
for Unices

BitDefender Antivirus Scanner for Unices
User's Guide

SOFTWIN

Published 2006.04.27
Version 1.24.1867

Copyright © 2006 SOFTWIN

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 SOFTWIN for the use of the SOFTWIN 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. SOFTWIN 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 SOFTWIN 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 SOFTWIN 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 SOFTWIN. 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. SOFTWIN 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 SOFTWIN replacing the faulty media, at its sole discretion, upon receipt of the said media, or refunding the BitDefender price. SOFTWIN does not warrant either the uninterrupted or error free operation of BitDefender or the correction of possible errors. SOFTWIN does not warrant that BitDefender will meet your requirements.

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, SOFTWIN 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. SOFTWIN 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 SOFTWIN 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 SOFTWIN 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 SOFTWIN'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 SOFTWIN. 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 SOFTWIN 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.

SOFTWIN 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 SOFTWIN shall prevail.

Contact SOFTWIN, at 5, Fabrica de Glucoza street, 72322-Sector 2, Bucharest, Romania, or at Tel No: 40-21-2330780 or Fax:40-21-2330763, e-mail address: <office@bitdefender.com>

Preface

This *User's Guide* is intended to all who have chosen BitDefender Antivirus Scanner for Unices as security solution for their systems. The information presented in this book is suitable not only for computer literates, it is accessible to everyone who is able to do administrative tasks on a Linux box.

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

We wish you a pleasant and useful lecture.

1. Conventions used in this book

1.1. Typographical conventions

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

Appearance	Description
variable	Variables and some numerical data are printed with monospaced characters.
http://www.bitdefender.com	The URL links is pointing to some external location, on http or ftp servers.
<support@bitdefender.com>	Emails are inserted in the text for contact information.
Chapter 5 "*Package installation*" (p. 33)	This is an internal link, towards some location inside the document.
filename	File and directories are printed using monospaced font.

Appearance	Description
`ENV_VAR`	The environment variables are `MONOSPACED CAPITALS`.
emphasized	The *emphasized text* is specially marked to require your attention.
"quoted text"	The quoted text is provided as reference.
command	Inline commands are printed using **strong** characters.
`# command -parameter`	Command examples are printed with strong monospaced characters in specially marked environment. The prompt can be one of the following.
	# The root prompt. You should be root in order to run this command.
	$ The normal user prompt. You do not need special privileges to run the command.
`screen output`	The screen output and code listings are printed with monospaced characters in specially marked environment.

1.2. Admonitions

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

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

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

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

2. The book structure

The book consists of four parts, containing the major topics: Description and features, Installation, Usage and Getting help. Moreover, a glossary and UNIX manual pages are provided to clarify some different aspects of BitDefender, which could issue technical problems.

Description and features. A short introduction to BitDefender. It explains who is BitDefender, who is SOFTWIN and Data Security Division. You are presented BitDefender Antivirus Scanner for Unices, its features, the product components and the basics of the integration and the filtering mechanism.

Installation. Step by step instructions for installing BitDefender on a system. Starting with the prerequisites for a successfully installation, you are conducted through the whole installation process. Finally, the uninstall procedure is described in case you need to uninstall BitDefender.

Using BitDefender. Description of basic administration and maintenance of BitDefender. You are presented the BitDefender configuration file, how to get run-time information, how to test the antivirus efficiency, how to perform the updates and how to register the product. You are also presented real life usage scenarios, covering various aspects of using BitDefender to detect malware on your system, and several desktop and server integration procedures, to have the antivirus scanning the files directly from the file manager or the emails passing your local email server.

Getting help. Where to look and where to ask for help if something goes not so right. You are guided to the Knowledge Base and offered the BitDefender and BitDefender partners contact information to call, if needed.

Manual pages. The manual pages of BitDefender Antivirus Scanner for Unices are included for a quick and convenient reference. Whenever you will find examples of BitDefender commands, the manual pages will provide you a valuable help to understand all the options and actions.

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 the best documentation possible.

Let us know by sending an email to <documentation@bitdefender.com>.

Description and features

Chapter 1. Overview

BitDefender provides security solutions to satisfy the protection requirements of today's computing environment, delivering effective threat management for over 41 million home and corporate users in more than 100 countries.

Designed to provide full protection for corporate network and systems, the BitDefender solution range comprises, beside antivirus protection, antispam, personal firewall and security management solutions. BitDefender also specializes in providing assistance with designing and establishing content security policies for corporate networks.

BitDefender Professional was the third product of its kind in the world to receive ICSA certification for Windows XP and the first to be awarded for groundbreaking innovation by the European Commission and Academies. BitDefender Antivirus is certified by all the major reviewers in the antivirus field - ICSA Labs, CheckMark, CheckVir, TÜV and Virus Bulletin.

BitDefender is headquartered in Bucharest, Romania and has offices in Tettnang, Germany, Barcelona, Spain and Florida, US. Website: http://www.bitdefender.com

1.1. Why BitDefender?

Proven. Most reactive antivirus producer. BitDefender fast reactivity in case of computer virus epidemic was confirmed beginning with the last outbreaks of CodeRed, Nimda and Sircam, as well as Badtrans.B or other dangerous, fast-spreading malicious codes. BitDefender was the first to provide antidotes against these codes and to make them freely available on the Internet for all affected people. Now, with the continuous expansion of the Klez virus - in various versions immediate antivirus protection has become once more a critical need for any computer system.

Innovative. Awarded for innovation by the European Commission and EuroCase. BitDefender has been proclaimed a winner of the European IST-Prize, awarded by the European Commission and by representatives of 18 academies in Europe. Now in its eighth year, the European IST Prize is a reward for groundbreaking products that represent the best of European innovation in information technology.

Comprehensive. Covers every single point of your network, providing complete security. BitDefender security solutions for the corporate environment satisfy the protection requirements of today's business environment, enabling management of

all complex threats that endanger a network, from a small local area to large multi-server, multi-platform WAN's.

Your Ultimate Protection. The final frontier for any possible threat to your computer system. As virus detection based on code analysis has not always offered good results, BitDefender has implemented behavior-based protection, providing security against born-new malware. MIDAS (Malware Intrusion Detection Advanced System), featuring three levels of security, guarantees your serenity even after the fastest epidemics.

These are **the costs** that organizations want to avoid and what the security products are designed to prevent:

• Worm attacks
• Communication loss because of infected e-mails
• E-mail breakdown
• Cleaning and recovering systems
• Lost productivity experienced by end users because systems are not available
• Hacking, and unauthorized access that causes damage

Some simultaneously **developments and benefits** can be accomplished by using the BitDefender security suite:

• Increase network availability by stopping the spread of malicious code attacks (i.e., Nimda, Trojan horses, DDoS).
• Protect remote users from attacks.
• Reduce administrative costs and deploys rapidly with BitDefender Enterprise management capabilities.
• Stop the spreading of malware through e-mail, using a BitDefender e-mail protection at the company's gateway. Temporarily or permanently block unauthorized, vulnerable, and expensive application connections.

1.2. Data Security Division

Ever since the beginning, SOFTWIN's Data Security Division approached data protection in a specific manner, with the first intelligent update, requiring no user intervention, the first remote antivirus management through WAP technology or the first Personal Firewall to be integrated within an antivirus engines to provide complete response to today's complex security threats.

Born to provide full data security at all critical levels in today's business environment, Data Security Division aims to ensure the protection of systems against computer

viruses, to do antivirus research, to develop new technologies for monitoring all possible ways to infect a system and, last but not least, to educate the IT&C public on the danger of computer viruses.

BitDefender security solutions satisfy the protection requirements of today's business environment, enabling management of all complex threats that endanger a network, from a small local area to large multi-server, multi-platform WAN's.

1.3. SOFTWIN

Bucharest-based SOFTWIN is the leading provider of complex software solutions and services in Romania.

SOFTWIN focuses on providing software solutions and services that enable fast growing companies to solve critical business challenges and to capitalize on new business opportunities.

SOFTWIN enables companies to focus on their core business and expand to new markets, by outsourcing non-core activities.

SOFTWIN employs over 500 highly qualified professionals experienced in developing customized solutions and services.

Since its establishment in 1990, SOFTWIN's average annual revenue has increased by +30%.

SOFTWIN has 4 divisions, which also define the company's main business lines:

• Customer Relationship Management
• Business Information Solutions
• eContent Solutions
• Data Security Solutions

SOFTWIN provides services and solutions to customers worldwide. Over 90% of the company's turnover is achieved from exports to the US and European Union.

Using cutting edge technologies, SOFTWIN successfully developed over 500 software development projects, over 3,500 content structuring projects for international partners, having over 43 million data security solutions users in 80 countries worldwide and more than 1,500,000 client calls handled annually for CRM services.

Chapter 2. Product features

The acquisition and installation of an antivirus product for the personal or company's systems is the most efficient way of preventing the infection of a computer and the spreading of viruses inside the company, and outside the company as well.

2.1. BitDefender Antivirus Scanner for Unices

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

The on-demand scanner, 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 BitDefender scan engines advanced features, 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. This technology detects 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).

In case an infection is found, the file will be treated corresponding to the selected option (disinfection, deletion, isolation in the quarantine area or just reporting) and notifications will be sent to console, as well as to the log file.

For ensuring a superior and efficient antivirus protection, BitDefender Antivirus Scanner for Unices was designed with built-in update function.

2.2. Key Features

- Antivirus protection for the file system.
- Automatic and incremental update of virus definitions and scanning engines directly from BitDefender servers.
- Ability to isolate the infected files in the quarantine zone.
- Detailed statistics and reports regarding the number of scanned files, the infected files, the deleted and disinfected files.

Chapter 3. The 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 upon a distinctive code pattern. The BitDefender Antivirus engine database includes over 250000 different malware signatures, at the moment of this writing, and the number constantly increases every few hours.

For identifying the unknown viruses, the engines can perform the heuristic analysis, searching for several features characterizing the viruses.

The objects to be scanned can be directories or regular files, provided as command line parameters. After the object is eventually deployed in a temporary file, the engines are asked to start the scanning process.

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

- **Disinfect.** BitDefender will try to disinfect the object, by removing the infected or suspected part. The action can fail sometimes.
- **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, inside mail boxes and inside packed programs. If this behavior is not desirable, there are command line options to disable them selectively `--no-archive`, `--no-mail` and `--no-pack`, respectively.

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

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

Installation

Chapter 4. Prerequisites

BitDefender Antivirus Scanner for Unices can be installed on package based Linux distributions (rpm or deb) and tbz based FreeBSD versions, but also all the other distributions are supported, using a pseudo-package system, with the same functionality of the others. These packages are built as bzip2 compressed tars and 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.

4.1. System requirements

Before installing BitDefender Antivirus Scanner for Unices, you must verify that your system meets the following system requirements.

4.1.1. Hardware system 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 32MB, recommended is 64MB, for a better performance.

Free disk space
The minimum free disk space to install and run BitDefender Antivirus Scanner for Unices is 4MB. But the log and the quarantine directory 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 some proxy server. Therefore, for an up to date protection, the Internet connection is a MUST.

4.1.2. Software system requirements

Linux requirements

The Linux kernel should be 2.2, 2.4 or 2.6, the recommended one is 2.6, with support for a fast file system, which works well with multiple small files, such as ext3 or reiserfs.

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

FreeBSD requirements

The supported FreeBSD versions are 5.3-RELEASE and greater and 6.0-RELEASE and greater.

FreeBSD 4 is no longer supported.

4.2. Package naming convention

BitDefender Antivirus Scanner for Unices package is named considering the following scheme.

4.2.1. Linux convention

```
BitDefender-scanner-{ver}.{os}.{arch}.{pkg}
```

Variable	Description
`{ver}`	This is the package version. For example, 7.5-3 is version 7, subversion 5, package build 3.
`{os}`	The operating system is Linux.
`{arch}`	The architecture contains the processor class and gcc compiler version. i586 is the current development version.
`{pkg}`	This refers to the package management tool used to install the files. This is one of `rpm`, `deb` or `run`. `rpm` uses the Red Hat Package Manager, `deb` uses the Debian package system and `run` is a self-extractable archive, the most portable method. Please install the appropriate package for your system, as described in the next chapters.

4.2.2. FreeBSD convention

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

Where *{ver}* is the package version. For example, 7.5_3 is version 7, subversion 5, package build 3.

Chapter 5. Package installation

This chapter will explain you how to install BitDefender on a Unix-like system, such as Linux or FreeBSD. This is pretty straightforward: get the desired package, test it for integrity, then install it.

5.1. Getting BitDefender Antivirus Scanner for Unices

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

The Linux package come in three flavours.

• `rpm` for distributions using the RedHat Linux package management
• `deb` for distributions using Debian Linux packaging system
• `run`, a self-extractable archive, suited for any other distribution

The FreeBSD package is a tbz (.tar.bz) compressed archive, adequate for the versions 5 and 6.

5.2. Test the package for integrity

Before you begin the installation process we recommend you to check the installation kit is not corrupted (this can happen sometimes, especially if you downloaded it).

5.2.1. Test the rpm and deb packages

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

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

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

Then, export the key to a local file:

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

For the rpm packages, you have to import the key into rpm key ring, using the next command.

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

When you wish to check a 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 over the deb files.

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

5.2.2. Test the self-extractable archive

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

```
# ./BitDefender-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.

5.2.3. Test the FreeBSD tbz package

When installing the package downloaded from the BitDefender servers, you shoud run **md5sum** on the package and compare the output with the value from the md5sums file. This file is located in the same directory you have downloaded the package from.

When installing from the ports collection, the integrity is automatically checked.

5.3. Install the package

The installation process depends on the package type. There are different methods for `rpm`, `deb` and self-extractable archive, as well as a typical method for FreeBSD.

5.3.1. Install the rpm package

To install BitDefender Antivirus Scanner for Unices on a RedHat based distribution, using the RedHat package manager, you have to run the following command.

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

5.3.2. Install the deb package

To install BitDefender Antivirus Scanner for Unices on a Debian based distribution, using **dpkg**, you have to run the following command.

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

5.3.3. Install the self-extractable archive

The self-extractable archive is a package containing all the required files for the installation. It acts as a shell script (you can open it with a text editor) and can be given several parameters in the command line. Usually, for a normal installation, there are no parameters required, simply run the script.

Run the self-extractable archive

This package should be installed using the following command.

```
# ./BitDefender-scanner-{ver}.{os}.{arch}.run
```

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

Additional parameters

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

Parameter	Description
--help	Prints the short help messages.
--info	This will print 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	This option will print 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 comparing the embedded md5 checksum (generated during packaging) with the one computed the moment of checking. If they match, the output will be the following:
	
	`MD5 checksums are OK. All good.`
	
	If not, an error message will be shown, displaying the unequal 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.

Parameter	Description
--uninstall	Run the embedded uninstaller script instead of the normal installer. For uninstalling, please read more in Chapter 6 "*Uninstall*" (p. 39).

5.3.4. Install the FreeBSD package

To install BitDefender Antivirus Scanner for Unices on a FreeBSD machine, you have two methods: you can install the package you have downloaded from the BitDefender servers or you can install from the ports collection.

Install a locally downloaded package

To install a local downloaded package, run the next command in its directory.

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

Install from the ports collection

To install from the ports collection, you have to run the following commands.

```
# cd /usr/ports/security/bitdefender-bdscan
# make install clean
```

5.4. The installer

After unpacking the archive, the installer is launched. This is a text based installer, created to run on very different configurations. It's purpose is to install the extracted packages to their locations and to make the first configuration of BitDefender Antivirus Scanner for Unices, asking you few questions. To accept the defaults the installer offers (which is recommended), you only have to 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 agree 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 the License Agreement and the installation process will stop.

Next, the *Installation directory* is asked, if you have installed BitDefender Antivirus Scanner for Unices on Linux, using the self-extracting archive. The default is `/opt` and we will assume you go for it. The installer will create the directory `/opt/BitDefender-scanner`, which will be the top-level directory on BitDefender Antivirus Scanner for Unices, containing several sub-directories, such as `doc`, `man`, `var`, `Plugins` (which is the location of the engines) and program binaries and the configuration file. If the above-mentioned directory does not exist, you are asked whether the installer should create it, assuming the default *yes*. If you do not agree the directory to be created, the installer will stop.

From this moment, the installer has acquired all the necessary information and will begin the install process. Basically, it will install the engines, the binaries and the documentation and 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 `bdscan` command in `/usr/bin/bdscan` for Linux and `/usr/local/bin/bdscan` for FreeBSD
- configures the quarantine directory

Chapter 6. Uninstall

If you ever need to remove BitDefender Antivirus Scanner for Unices, there are several methods to do it, depending on the package type.

6.1. Uninstall the rpm package

To uninstall BitDefender Antivirus Scanner for Unices on a RedHat based distribution, using the RedHat package manager, you have to run the following command.

```
# rpm -e BitDefender-scanner
```

6.2. Uninstall the deb package

To uninstall BitDefender Antivirus Scanner for Unices on a Debian based distribution, using **dpkg**, you have to run the following command.

```
# dpkg -r BitDefender-scanner
```

6.3. Uninstall using the self-extractable archive

To proceed, you need the original self-extractable install archive and use the method described below. This is necessary since the program will automatically undo all the settings used for integration with the system.

All you have to do is to run the following command.

```
# ./BitDefender-scanner-{ver}.{os}.{arch}.run --uninstall
```

First, the installation directory is requested from you. By default, it should be /opt, but if you have selected another one during the installation, you have to specify it when asked. The uninstall program will check whether the directory is correct, by verifying whether bdscan file exists inside of it. If there is something wrong, the uninstall will quit.

Next, the uninstall procedure begins by removing installation directory, /opt/BitDefender-scanner. The MANPATH environment variable is restored to its previous value. Finally, the /usr/bin/bdscan symlink is deleted. At this moment, the system should be left in the same condition as found before installing.

6.4. Uninstall the FreeBSD package

To uninstall the FreeBSD package, you have two methods, according to the installation way.

6.4.1. Uninstall a package downloaded locally

To uninstall a package you have installed form a local download, run the next command.

```
# pkg_delete bitdefender-scanner
```

6.4.2. Uninstall from the ports collection

To uninstall the package installed from the ports collection, you can use the previos method or run the following commands.

```
# cd /usr/ports/security/bitdefender-bdscan
# make deinstall clean
```

Using BitDefender

Chapter 7. The 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/bdscan.conf` on FreeBSD systems. There is another configuration file, located inside the user's home directory, at `~/.BitDefender/bdscan.conf`, which is loaded after the system configuration. Therefore, the user can specify settings to override partially or even totally the system settings.

> **System versus User configuration**
>
> In this book we will talk about changing the system-wide configuration file, but remember that you can modify the user's own configuration, with the same effect from his point of view.

The files are standard UNIX-style configuration files, based on pairs `key=value`, 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 the home directory, in
# ~/.BitDefender/bdscan.conf and change the settings to suit their
# need. 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/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 could not be present at a certain moment, since their default values, defined internally, may need no change.

Key	Description
InstallPath	This is the path to 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 73) for more information about updates and proxy configuration.

Key	Description
QuarantinePath	This is the location of the quarantine directory, where the infected files are stored when quarantine actions are invoked.
	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 has not 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 sent normally to `STDOUT`. The new log will be appended to the end of the last one on new scan. If you want to clear the log file before scanning, you have to use `--log-overwrite` command line option.
	The log file can be also 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 has not the right to write it, the location becomes `~/.BitDefender/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.
ExcludeExtensions	This list, with colon-separated items, specifies the file types to exclude from scanning, identified by their extensions.

Key	Description
	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.

> **ⓘ Product registration**
> Please see Chapter *Product registration* (page 77) for more information about license keys.

Chapter 8. Testing BitDefender

You can verify that BitDefender Antivirus component works properly with the help of a special test file, known as *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 within 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 puts a 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*
```

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

> **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.

8.1. Scan an executable file

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

```
# bdscan EICAR.COM
```

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

The command output will be the following.

```
BitDefender Antivirus Scanner v7.60124 Linux-i686
Copyright (C) 1996-2006 Softwin 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
```

8.2. Scan an archive

Next, you could archive or compress the file and run **bdscan** over it. BitDefender will scan inside the archive.

First, let's use the **gzip** command to create the compressed file. Of course, you can use several other tools, such as **zip**, **rar**, **arj** and so on.

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

Now you can run **bdscan** over this compressed file.

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

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

```
BitDefender Antivirus Scanner v7.60124 Linux-i686
Copyright (C) 1996-2006 Softwin 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
```

8.3. 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 next example.

```
# bdscan mail.mbox
```

The email messages from the mailbox are read one by one, the attachments are unpacked, the contents are extracted and finally scanned. BitDefender will display the subject of the infected email, its date and the infected attachments.

```
BitDefender Antivirus Scanner v7.60124 Linux-i686
Copyright (C) 1996-2006 Softwin 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
```

Chapter 9. Real life usage

These are some real-life usage examples of BitDefender. Use them as guidelines for improving your system protection and, 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>.

9.1. Virus scanning

BitDefender Antivirus Scanner for Unices knows the best how to perform an antivirus scan on files and directories located on some filesystem. Here are some basic usage examples.

9.1.1. 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 the file was moved to quarantine directory. Since verbose messages were asked, the name of the plugins used are also displayed.

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

Of course, you can use the ignore action (which is equivalent to 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) 1996-2006 Softwin 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
```

9.1.2. Scan a directory

The path to scan can be not only a path towards some file, but to any directory. BitDefender Antivirus Scanner for Unices can scan recursively a directories tree, with unlimited recursive level. You can change this, by setting a fixed depth level or by disabling the recursion at all.

Let's suppose we have the following tree structure, with one file and two sub-directories, each sub-directory containing some other files.

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

We want to scan the downloaded_files directory, but not the sub-directories, therefore the recursion level is 1. We also want to quarantine the infected files, to study them later.

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

The next screen output shows the files scanned, found infected and finally quarantined. You can notice the two sub-directories were not scanned.

```
BitDefender Antivirus Scanner v7.60124 Linux-i686
Copyright (C) 1996-2006 Softwin 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
```

9.1.3. Scan the entire system

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

The only problem is the number of files to be scanned and the time to scan them, which could be very long, depending on your system's performance and filesystem's capacity. Therefore you could use a log file (to analyze after the scanning process has finished) and to reduce the screen output, displaying only the infected and the suspected files.

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

Only the found malware 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 the report regarding them.

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
...
```

9.1.4. Scan the archives

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

⚠️ **Actions on archives**
You should be aware of the fact that some actions, such as `disinfect`, are possible to fail when scanning archives. The reason is BitDefender will not try or will not succeed to recreate the archive, removing some objects from inside. Several closed-source compression algorithms are free only to uncompress and 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 recursive level, with the next 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 see also which engine process each step of unpacking and scanning.

```
BitDefender Antivirus Scanner v7.60124 Linux-i686
Copyright (C) 1996-2006 Softwin 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
```

9.1.5. Scan the mailbox

If you want to scan your mailbox, or just some emails, you can run BitDefender Antivirus Scanner for Unices on them. Each email from a mailbox will be treated separately, the attachments will be extracted and scanned. The list of scanned objects can get very large, so you could use the logfile facility.

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

This example shows how an email message from a mailbox, containing a compressed attachment, is scanned and the attached file is found infected.

```
BitDefender Antivirus Scanner v7.60124 Linux-i686
Copyright (C) 1996-2006 Softwin 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 ... OO (EEST)]=>(MIME part)  ok <- mime.xmd
/tmp/mail.mbox=>(messag ... E part)=>(message body)  ok <- mime.xmd
/tmp/mail.mbox=>(messag ... OO (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 ... OO (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
```

9.2. Report

You can ask BitDefender to show various kind of information regarding its activity,
status, known viruses or version.

9.2.1. Using the log file

BitDefender can run in background with no user intervention, can display an enormous
quantity of information or you would like to keep its activity reports for a later use. In
these cases, the best way is to use the log facility.

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

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

9.2.2. Get more information

BitDefender can offer some information about scanning engines, last update, key validity, etc. when called with --info command line option.

```
# bdscan --info
```

You will get the next screen output.

```
BitDefender Antivirus Scanner v7.60124 Linux-i686
Copyright (C) 1996-2006 Softwin 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
```

9.2.3. Display the virus list

BitDefender can send to STDOUT its virus list, which is really big. To study it, you have to 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
```

Now, you can navigate inside the list or search for some virus name, using the pager's facilities.

9.2.4. Display the product version

Maybe you will need just to find the version of your installed BitDefender Antivirus Scanner for Unices.

```
# bdscan --version
```

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

```
BitDefender Antivirus Scanner v7.60124 Linux-i686
Copyright (C) 1996-2006 Softwin SRL. All rights reserved.
```

9.3. Virus submission

Sometimes, BitDefender will not present files as *infected*, but *suspected*. The suspected files have not matched any signature, but the heuristic analysis marked them as possibly infected. Usually, they should be moved to quarantine directory and submitted to BitDefender Antivirus Lab at <virus_submission@bitdefender.com> for a deeper analysis.

These emails can trigger some antiviruses on email servers in their way to BitDefender Antivirus Lab, therefore you have to compress them in an encrypted zip archive and send both the archive and the password in the same email.

For example, you can use the command below.

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

You will be prompted twice for a password. Pick a simple one, as the encryption is only used for scrambling the file, not for protecting it.

Chapter 10. BitDefender integration

BitDefender Antivirus Scanner for Unices is a versatile antivirus scanning solution, that could be easily integrated in desktop and server software to perform an instant target scan.

10.1. Desktop integration

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

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

10.1.1. Midnight Commander

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

The user menu, invoked with **F2** key, represents an easy way to provide users a menu to add extra features to the Midnight Commander. This can be edited by selecting from the menus **Command → Menu file edit**. You will be asked whether to edit the **Local** or the **Home** menu; select to edit the **Home** menu, for changes to be available in any directory.

The menu file is opened in an editor. Go to the end of the file and append the following lines. The care to respect the white spaces from the beginning of the lines.

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

> ℹ️ **Different installation path**
> If you have used another installation path and not the default one, please change the first line accordingly. That condition is used not to show the menu item if BitDefender Antivirus Scanner for Unices is not installed.

From now on, when you press the **F2** key on top of some tagged or not tagged files and directories, the User menu pops-up and by pressing the **S** key you will perform an antivirus scan of the target.

When scanning, 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.
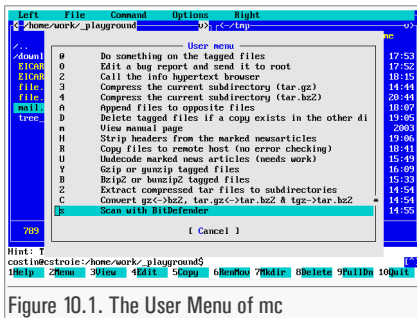
Figure 10.1. The User Menu of mc

10.1.2. KDE Konqueror

Konqueror is the file manager for the K Desktop Environment. Using a special 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, since 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 will close it.
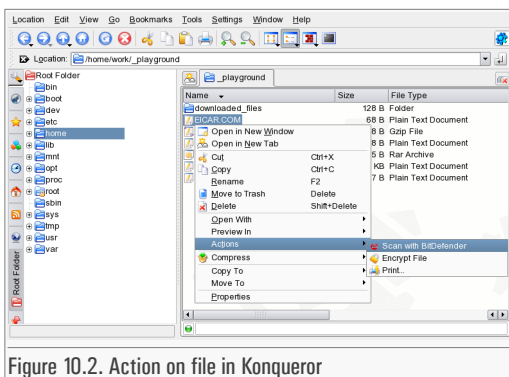
Figure 10.2. Action on file in Konqueror

10.1.3. 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 from Section *KDE Konqueror* (page 60).

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 tab **User Actions** 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 check **Execution mode → Run in terminal** checkbox.

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

Now, in the **Useractions** menu there will be a new item, **Scan with BitDefender**. Select it to start scanning the targeted files and directories.

The program output will be displayed in a console window, that will not close when the scanning process finishes. You will have to close it manually, after reading the messages.
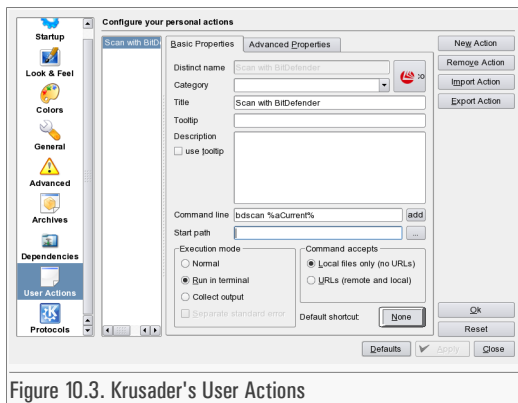
Figure 10.3. Krusader's User Actions

10.1.4. 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 directory `~/.rox_choices/SendTo/`.

```
#!/bin/sh
# BitDefender ROX-Filer integration script
# Copyright (C) 1996–2006 SOFTWIN 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 finished, you will need to close the window, after reading the output messages.

10.1.5. Pine

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

To scan an email from some mail user agent, you have to save the message on the filesystem and scan that file. Fortunately, these actions can be automated, by using a shell script. Save the following file to some 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) 1996-2006 SOFTWIN 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
```

What to do with infected emails

You will not be able to disinfect the message, the only action that can be done is `ignore`, therefore it's up to you to delete or move the email if BitDefender has found it infected or, better, instruct the email client to do so.

If you want to be able to scan emails from Pine using BitDefender, you have to change your Pine settings to enable Unix pipe commands. 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 email, there is one more command: **| Pipe**, ready to be tested.

1. When displaying a message or in the Index screen, press the **| Pipe** key (**Shift**+****).
2. The entire message has to 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`, and press **ENTER**.

This is how the screen should look like.

```
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 email will be piped to BitDefender filter, which will save it temporary on the filesystem and scan this file with **bdscan**. After the scan, the output results are

displayed by Pine. You should notice whether the email was infected or not. When finished reading the messages, press **E** to Exit the viewer.

As stated before, it would be better to tell Pine to automatically scan the messages and what to do when some infected email is found. This way, every new message will be scanned and treated accordingly, meaning that the message displaying will slow down a bit.

Possible actions to do on infected email could be the following.

- Set a keyword (let's say `Infected`) and add an IndexColor rule to highlight the message with this keyword.
- Move the email to some safe location, to study it carefully.
- Remove the email.

We will discuss how to create a filter rule to move the infected email to another mailbox.

Type **S** (for Setup), then **R** (for Rules) and **F** (for Filters). Then press **A** (Add) to add a new rule. First, give it a name, such as *BitDefender Antivirus Scan*, then check **Current Folder Type → Email** to apply the rule on all email folders. Furthermore, you can also check **Message is New (Unseen)? → Yes**, to scan only new emails, increasing the speed.

Scroll down to **External Categorizer Commands** and set the following values.

- **Command**: /opt/BitDefender-scanner/bin/bdscanpipe
- **Exit Status Interval**: (1,254)

Scroll down to **Filter Action** and select **Move**. You have to specify the folder to move the infected email to.

Finally, check **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 email is received, it will piped to BitDefender filter and, depending on the exit status, it will be moved to some safe location if found infected.

10.1.6. 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*

Making Evolution scan emails through BitDefender can be accomplished by using the email Filters. This way, when you download any new message, it will be sent to scanning.

> **(i)** BitDefender pipe: bdscanpipe
>
> Evolution needs a filter to pipe the messages into. Please review the Section *Pine* (page 63) and use the provided script.

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

Next, in the **Then** panel, you will set the action to do on infected email. For example, you could move it to some special folder (name it *Infected*), you could set some color or just delete the message.

From now on, any new email will be piped into the scanning filter. If you want to scan only some emails, add corresponding rules to

Figure 10.4. Evolution filter configuration

If panel. For manually scanning some highlighted message, press **Control**+**Y** keys.

10.1.7. KMail

KMail is a fully-featured email 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

KMail integration can be done using the wizard from **Tools → Anti-virus Wizard...** menu. This will autodetect BitDefender and will automatically configure the filters to pipe any message through a script that will add a header to the message, X-Virus-Flag with values Yes or No, depending on the email is infected or not.

If you do not like to use the wizard, you can add manually the filter rule. Start from **Settings → Configure filters...**. Add a new filter and name it *BitDefender Anti-Virus Check*. In the **Filter Criteria** panel add a rule to select which messages to scan, for example a rule that will scan all messages. In the **Filter Actions** panel select **Pipe Through** and fill in the textbox kmail_bitdefender.sh. Then check the boxes **Apply to incoming message** and **Apply on manual filtering**. Save the new rule by pressing the **OK** button.

Figure 10.5. KMail filter configuration

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

```
#!/bin/sh
# BitDefender KMail integration script
# Copyright (C) 1996-2006 SOFTWIN 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_$$
```
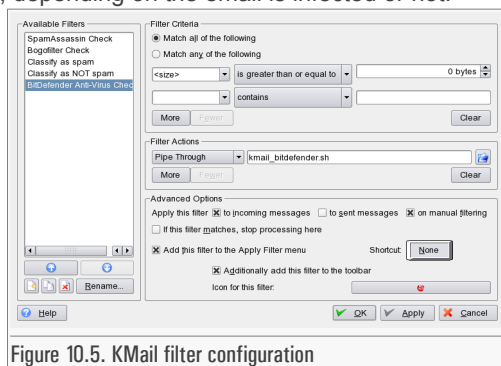
```
# Save the standard-input to a temporay file
cat > $TMPFILE

# 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
```

Even more, you can customize by yourself this filter. You can add a convenient button on the toolbar, to call the filter on the highlighted message.

Filter actions in KMail
Due to the current KMail structure, the script is called in the **Actions** section on the filter. That means the only action the filter can do is to add a header stating 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.

10.2. Server integration

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

10.2.1. 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 some option to the script, such as specifying the antivirus to use.

Qmail-Scanner installation
Qmail-Scanner supports many installation options, for a fine-grained qmail integration. Please see 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 configured, you can install Qmail-Scanner by running the next command.

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

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

10.2.2. MailScanner

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

MailScanner integration of BitDefender is a very simple process. Since BitDefender Antivirus Scanner for Unices is supported by default by MailScanner, all you need to have is a functional installation of MailScanner and one line to modify.

MailScanner installation
Please refer to on-line or printed MailScanner documentation for a detailed view of installation, since this is out of the subjects covered by this book.

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 next line.

```
Virus Scanners = none
```

Change it to the following form.

```
Virus Scanners = bitdefender
```

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

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

Before real usage, it would be better to check BitDefender was properly detected. Therefore, run the next command and watch for the line saying bdscan has been found.

```
# amavisd-new debug
```

Somewhere in the output, you will see the next line.

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

This is all you have to do. You can now test the mail server integration using EICAR emails.

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

Chapter 11. Updates

BitDefender Antivirus Scanner for Unices was designed with capabilities for triggered update. At the present time, the risk of getting infected is high, both because new viruses appear and the existing ones keep on spreading. This is why your antivirus must be kept up-to-date, by periodically checking the BitDefender servers for new updates.

11.1. Triggered update

11.1.1. Run the triggered update

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

```
# bdscan --update
```

The output should be the following.

```
BitDefender Antivirus Scanner v7.60124 Linux-i686
Copyright (C) 1996-2006 Softwin 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.
```

11.1.2. Regular updates

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

Edit the cron table

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

```
# crontab -e
```

Then add the next 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 next command 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
```

This way, you will run the update every night at 2:00 AM.

Use cron.* scheduling facility

Depending on you Linux distribution, there could be another method for regular updates. Most of the major distributions use **cron** to run some 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 **cron** new job or to remove it.

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 following file, name it bdscan-update and place it in the selected directory. Do not forget to change the INSTALL_PATH according to your installation, if you have not installed under default location.

```
#!/bin/sh
# BitDefender update script, using cron service
# Copyright (C) 1996-2005 SOFTWIN 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 with the next command.

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

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

11.1.3. HTTP proxy

You may use a HTTP proxy server to connect to Internet. In this case, the triggered update may fail, since the BitDefender update server can not be reached.

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

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

11.2. Manual update

If you have no Internet access, meaning that **bdscan** can not check and download the updates, you can perform a manual update. Basically, there are two zip archives

on the update server, containing the updates of the scanning engines and virus signatures: `cumulative.zip` and `daily.zip`.

- `cumulative.zip` is released every week on Monday and it includes all the virus definitions and scan engines updates up to the release date.
- `daily.zip` is released each day and it includes all the virus definitions and scan engines updates since the last cumulative and up to the current date.

In order to update the product manually, you should follow the next steps.

1. **Download the updates files.** If it is Monday, please download the `cumulative.zip` and save it somewhere on your disk when prompted. Otherwise please download the `daily.zip` and save it on your disk. If this is the first time you update using the manual updates, please download the both archives.
2. **Extract the updates.** Extract the contents of the zip files to `/opt/BitDefender-scanner/var/lib/scan/Plugins/` directory, overwriting the existing files with the newer ones if necessary.

> **The order to extract the updates**
> If you are using both update files, you will have to extract the content of the `cumulative.zip` first, then the contents of `daily.zip`.

3. **Set files owner and permissions.** After extracting the zip archives, you **must** set the proper owner and permissions, by running the following commands.

```
# chown root:root /opt/BitDefender-scanner/var/lib/scan/Plugins/*
# chmod 644 /opt/BitDefender-scanner/var/lib/scan/Plugins/*
```

Chapter 12. 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 from `/etc/BitDefender-scanner/bdscan.conf` (for a default Linux installation) or from `/usr/local/etc/bitdefender/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 the expiration date**
> If you want to check the key expiration date, you have to run the following command and watch the output.
>
> ```
> # bdscan --info
> ```

12.1. Trial License

The product comes by default with a trial key which allows the user to use it in any way or any environment whatsoever for 30 days from the install time. When the trial period expires, all 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 one from the nearest BitDefender dealer.

12.2. License for home or personal use

This license is free and can be retrieved from the BitDefender website after filling a short form. It allows the user to use the product only for personal use with no

commercial implications whatsoever. For example, using the Personal License, you are allowed to scan your personal laptop or desktop computer but YOU ARE NOT ALLOWED TO USE IT IN A PRODUCTION ENVIRONMENT LIKE AN OFFICE COMPUTER OR COMPANY SERVER.

12.3. License for commercial use

If you plan on using BitDefender Antivirus Scanner for Unices with your own integration system or pre-designed scripts, then 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.

Chapter 13. Best practices

These are some steps you should follow to ensure a system free from viruses.

1. After installing BitDefender Antivirus Scanner for Unices, perform a triggered update to have the latest virus signatures and engines, as described in Section *Triggered update* (page 73).
2. Perform a full system scan to find any already infected objects. Use the guidelines from Chapter *Real life usage* (page 51).
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 77).
4. If you use **cron** or something else to do regular updates, make sure the job scheduler really works and you have always the latest updates.
5. When using the `quarantine` action, so the infected objects are moved to quarantine directory, keep one eye on it. Check periodically the directory size, since it can grow rapidly and you could run out of disk space, and 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, by web browsing or email. Scan the documents, archives, programs and anything else that could contain malicious code. Periodically, perform a full system scan.
7. Send to BitDefender Antivirus Lab at email address <`virus_submission@bitdefender.com`> all suspected objects for a prompt response to malware threats. To not be filtered by antivirus protected email servers, you can archive the suspected object, encrypt the archive and send both the archive and the key.

Getting help

Chapter 14. Frequently Asked Questions

1. Installation

1. What are the system requirements?

   Please consult for an up to date system requirements.

2. Does BitDefender alter my system configuration?

   Yes, BitDefender Antivirus Scanner for Unices will touch several system files (`man.config` and `manpath.config`) if found on the system, for manpage integration. It will also create certain symlinks in `/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, though I know that the file can be disinfected. Why does not it disinfect the file?

   The `--action` command line option, with value `ignore` by default, can be used to specify what to do when a virus is found. Possible values are `disinfect`, `delete`, `quarantine` or `ignore`.

   Also, note that there are lots of viruses, so called *malware*, which can not be disinfected, because of their internal structure and behavior, so if **bdscan** finds such a malware, it is recommended to delete the infected file.

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

   Run the following command and look for the line displaying the time of the last update.

   ```
   # bdscan --info
   ```

If you have BitDefender Antivirus Scanner for Unices performing a regular update, this time should be recent enough. If not, this is a good moment to update you antivirus.

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

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

There is really no update available at that time, especially if you are running the update very, very often.

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

New updates are released as soon as new malwares are 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 quarantine zone, I get a "move failed" in the log file. Why?

Make sure you have the proper rights on the quarantine directories, i.e. the directories must be writable for the users 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 use the quarantine facility, make sure to check from time to time those directories, and delete all unneeded files, to free up disk space.

6. Why **bdscan** does not scan symbolic links?

bdscan does not follow the symbolic links, neither for files, nor for directories. This behavior avoids unauthorized disk access and also the recursive loops, especially for `/dev` and `/proc` directories.

Chapter 15. Support

15.1. Support department

As a valued provider, SOFTWIN strives to provide its customers with an unparallel level of fast and accurate support. The Support Center listed below is continually being updated with the newest virus descriptions and answers to common questions, so that you obtain the necessary information in a timely manner.

At SOFTWIN, dedication to saving its customers time and money by providing the most advanced products at the fairest prices has always been a top priority. Moreover, we think that a successful business is based on a good communication and a commitment to excellence in customer support.

You are welcome to ask for support at <`support@bitdefender.com`> any time. For a prompt response, please include in your email as many details as you can about your BitDefender, about your system and describe the problem as accurate as possible.

15.2. BitDefender Knowledge Base

The BitDefender Knowledge Base is an online repository of information about 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 and detailed explanations, and many other articles.

The BitDefender Knowledge Base is open to the public and freely searchable. This welth of information is yet another way to provide 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 is available any time at http://kb.bitdefender.com.

15.3. Contact information

Efficient communication is the key to a successful business. For the past 10 years SOFTWIN has established an indisputable reputation in exceeding the expectations of clients and partners, by constantly striving for better communications. Please do not hesitate to contact us regarding any issues or questions you might have

15.3.1. Web addresses

Sales department: <sales@bitdefender.com>
Technical support: <support@bitdefender.com>
Documentation: <documentation@bitdefender.com>
Security reports: <security@bitdefender.com>
Product web site: http://linux.bitdefender.com
Product archives: http://download.bitdefender.com/linux
Local distributors: http://www.bitdefender.com/partner_list
BitDefender Knowledge Base: http://kb.bitdefender.com

15.3.2. Address

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

Germany

Softwin GmbH
Karlsdorfer Straße 56 88069
Tettnang
Technischer Support: <support@bitdefender.de>
Vertrieb: <vertrieb@bitdefender.de>
Phone: 07542/94 44 44
Fax: 07542/94 44 99
Product web site: http://www.bitdefender.de

Spain

Constelación Negocial, S.L
C/ Balmes 195, 2ª planta, 08006
Barcelona

Soporte técnico: <soporte@bitdefender-es.com>
Ventas: <comercial@bitdefender-es.com>
Phone: +34 932189615
Fax: +34 932179128
Sitio web del producto: http://www.bitdefender-es.com

U.S.A

BitDefender LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33308
Technical support: <support@bitdefender.us>
Sales: <sales@bitdefender.us>
Phone: 954 776 62 62, 800 388 80 62
Fax: 954 776 64 62, 800 388 80 64
Product web site: http://www.bitdefender.us

Romania

SOFTWIN
5th Fabrica de Glucoza St.
PO BOX 52-93
Bucharest
Technical support: <suport@bitdefender.ro>
Sales: <sales@bitdefender.ro>
Phone: +40 21 2330780
Fax: +40 21 2330763
Product web site: http://www.bitdefender.ro

Manual Pages

bdscan

bdscan — BitDefender Antivirus Scanner for Unices

Synopsis

bdscan [--action= disinfect | quarantine | delete | ignore] [--no-archive] [--no-mail] [--no-pack] [--no-recursive] [--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] [--virus-list] [--info] [--version] [--help] path-to-scan

Description

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

BitDefender Antivirus Scanner for Unices is mainly used to do file scanning, in order to find any kind of viruses, trojans, worms or malwares. It uses the most advanced scanning engine technology to provide high rates of detection, reliability and speed.

The user can choose to move the infected and suspected files to quarantine directories, disinfect or delete the files. **bdscan** has also 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.

--recursive-level=*level*
> Set the maximum recursive level to *level*. The default is 0, meaning no limitation.

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

--ext[=*ext1:ext2*]
> Specifies that **bdscan** should scan only the files with extensions specified in the list or in the configuration file, under the Extensions keyword.

--exclude-ext[=*ext1:ext2*]
> Specifies that **bdscan** should exclude from scanning the files with extensions 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*
> Set the quarantine directory, where the infected files are stored when the action is quarantine. If the user can not write into the quarantine directory, bdscan will exit with error when quarantine action is invoked.

--conf-file=*file*
> Set the alternate location of the configuration file. If this file is not valid, valid, bdscan will exit with an error message. By default, the configuration is read from /etc/BitDefender-scanner/bdscan.conf /usr/local/etc/bitdefender/bdscan.conf and ~/.BitDefender/bdscan.conf, the user file overrides partially or entirely 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, an error message will be output and the default one will be used. The default is ~/.BitDefender/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. The warnings are displayed in case a 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.

--virus-list
  Display the virus list. This could lead to lot of information to be displayed.

--info
  Print information about version, the current number of virus signatures, the moment of the last update, the number of scan engines, archive engines, unpack engines, mail engines and system engines.

--version
  Display a short message containing the version information and the copyright note.

--help
  Display the help message.

Actions

When an infected object is found, **bdscan** can be instructed to perform a specific action. These actions are the following.

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

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 /var/tmp directory, excluding
archives, to display detailed messages and to 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 /var/tmp directory, excluding
mailboxes, log its activity to /tmp/bdscan.log file and quarantine the infected files.

Files

/etc/BitDefender-scanner/bdscan.conf ,
/usr/local/etc/bitdefender/bdscan.conf ,
~/.BitDefender/bdscan.conf
>   The configuration files of **bdscan**. The system-wide configuration is overridden
>   by the user configuration.

Bugs

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

Also, there may be rare cases when **bdscan** crashes while doing file scan. If this is the case, you should update the scan engines and virus signatures and definitions.

See also

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

Glossary

ActiveX

ActiveX is a model for writing programs so that other programs and the operating system can call them. ActiveX technology is used with Microsoft Internet Explorer to make interactive Web pages that look and behave like computer programs, rather than static pages. With ActiveX, users can ask or answer questions, use push buttons, and interact in other ways with the Web page. ActiveX controls are often written using Visual Basic.

Active X is notable for a complete lack of security controls; computer security experts discourage its use over the Internet.

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.

98

Events

An action or occurrence detected by a program. Events can be user actions, such as clicking a mouse button or pressing a key, or system occurrences, such as running out of memory.

False positive

Occurs when a scanner identifies a file as infected when in fact it is not.

Filename extension

The portion of a filename, following the final point, which indicates the kind of data stored in the file.

Many operating systems use filename extensions, e.g. Unix, VMS, and MS-DOS. They are usually from one to three letters (some sad old OSes support no more than three). Examples include "c" for C source code, "ps" for PostScript, "txt" for arbitrary text.

Heuristic

A rule-based method of identifying new viruses. This method of scanning does not rely on specific virus signatures. The advantage of the heuristic scan is that it is not fooled by a new variant of an existing virus. However, it might occasionally report suspicious code in normal programs, generating the so-called "false positive".

IP

Internet Protocol - A routable protocol in the TCP/IP protocol suite that is responsible for IP addressing, routing, and the fragmentation and reassembly of IP packets.

Java applet

A Java program which is designed to run only on a web page. To use an applet on a web page, you would specify the name of the applet and the size (length and width--in pixels) that the applet can utilize. When the web page is accessed, the browser downloads the applet from a server and runs it on the user's machine (the client). Applets differ from applications in that they are governed by a strict security protocol.

For example, even though applets run on the client, they cannot read or write data onto the client's machine. Additionally, applets are further restricted so that they can only read and write data from the same domain that they are served from.

Macro virus

A type of computer virus that is encoded as a macro embedded in a document. Many applications, such as Microsoft Word and Excel, support powerful macro languages.

These applications allow you to embed a macro in a document, and have the macro execute each time the document is opened.

Mail client

An e-mail client is an application that enables you to send and receive e-mail.

Memory

Internal storage areas in the computer. The term memory identifies data storage that comes in the form of chips, and the word storage is used for memory that exists on tapes or disks. Every computer comes with a certain amount of physical memory, usually referred to as main memory or RAM.

Non-heuristic

This method of scanning relies on specific virus signatures. The advantage of the non-heuristic scan is that it is not fooled by what might seem to be a virus, and does not generate false alarms.

Packed programs

A file in a compression format. Many operating systems and applications contain commands that enable you to pack a file so that it takes up less memory. For example, suppose you have a text file containing ten consecutive space characters. Normally, this would require ten bytes of storage.

However, a program that packs files would replace the space characters by a special space-series character followed by the number of spaces being replaced. In this case, the ten spaces would require only two bytes. This is just one packing technique - there are many more.

Path

The exact directions to a file on a computer. These directions are usually described by means of the hierarchical filing system from the top down.

The route between any two points, such as the communications channel between two computers.

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 standards for how computers communicate and conventions for connecting networks and routing traffic.

Trojan
> A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.
>
> The term comes from a story in Homer's Iliad, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the

horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

Update

A new version of a software or hardware product designed to replace an older version of the same product. In addition, the installation routines for updates often check to make sure that an older version is already installed on your computer; if not, you cannot install the update.

BitDefender has it's own update module that allows you to manually check for updates, or let it automatically update the product.

Virus

A program or piece of code that is loaded onto your computer without your knowledge and runs against your will. Most viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can copy itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

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.

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com