



Bitdefender®

**Security for Mail
Servers**

ADMINISTRATOR'S GUIDE

Bitdefender Security for Mail Servers Administrator's Guide

Publication date 2021.07.19

Copyright© 2021 Bitdefender

Table of Contents

| | |
|---|-----------|
| Preface | vii |
| 1. Conventions Used in This Book | vii |
| 1.1. Typographical Conventions | vii |
| 1.2. Admonitions | ix |
| 2. Book Structure | ix |
| 3. Request for Comments | x |
| Description | 1 |
| 1. Features and Benefits | 2 |
| 1.1. Key Features | 2 |
| 1.2. Key Benefits | 2 |
| 2. Architecture | 4 |
| 2.1. Core Modules | 4 |
| 2.2. Integration Agents | 5 |
| 2.2.1. Sendmail | 6 |
| 2.2.2. qmail | 6 |
| 2.2.3. Courier | 6 |
| 2.2.4. CommuniGate Pro | 7 |
| 2.2.5. SMTP Proxy | 7 |
| 2.2.6. Postfix | 8 |
| 2.2.7. Exim | 9 |
| 2.2.8. Axigen | 9 |
| Installation | 10 |
| 3. Prerequisites | 11 |
| 3.1. System Requirements | 11 |
| 3.1.1. Hardware Requirements | 11 |
| 3.1.2. Software Requirements | 11 |
| 3.1.3. Internet Connection | 12 |
| 3.1.4. Mail Servers Minimum Required Versions | 12 |
| 3.2. Package Naming Convention | 12 |
| 4. Package installation | 14 |
| 4.1. Getting the Package | 14 |
| 4.2. Installing the Package | 14 |
| 4.2.1. Additional Parameters | 15 |
| 4.3. Initial Setup | 16 |
| 5. Uninstall | 18 |
| 5.1. Uninstalling the RPM Package | 18 |
| 5.2. Uninstalling the DEB Package | 18 |
| 5.3. Manual Uninstallation | 18 |

| | |
|---|----|
| Getting Started | 19 |
| 6. Start-up and Shut-down | 20 |
| 6.1. Start-up | 21 |
| 6.2. Shut-down | 21 |
| 6.3. Restart | 22 |
| 7. Bitdefender Status Output | 23 |
| 7.1. Process Status | 23 |
| 7.2. Basic Information | 23 |
| 7.3. Statistical Report | 24 |
| 8. MTA Integration | 25 |
| 8.1. CommuniGate Pro | 25 |
| 9. Basic Configuration | 27 |
| 9.1. View Settings | 27 |
| 9.2. Edit Settings | 32 |
| 10. Product Registration | 34 |
| Advanced Usage | 35 |
| 11. Configuration | 36 |
| 11.1. Group Management | 36 |
| 11.1.1. Adding and Editing Groups | 36 |
| 11.1.2. Integration with an LDAP Server | 38 |
| 11.1.3. Group Priority | 39 |
| 11.2. Antivirus Settings | 41 |
| 11.3. Antispam Settings | 43 |
| 11.3.1. X-Junk-Score Header for CommuniGate Pro Integration | 48 |
| 11.4. Content Filtering | 48 |
| 11.4.1. Examples | 50 |
| 11.5. The Bitdefender Logger Daemon | 54 |
| 11.5.1. The Logger Plugins | 55 |
| 11.6. Quarantine | 59 |
| 12. Third Party Integration | 62 |
| 13. Testing Bitdefender | 63 |
| 13.1. Antivirus Test | 63 |
| 13.1.1. Infected Email Attachment | 64 |
| 13.1.2. Infected Attached Archive | 64 |
| 13.2. Antispam Test | 65 |
| 14. Updates | 66 |
| 14.1. Automatic Update | 66 |
| 14.1.1. Time Interval Modification | 66 |
| 14.1.2. Bitdefender Live! Update Proxy Configuration | 67 |
| 14.2. Manual Update | 67 |

| | |
|--|----|
| 14.3. PushUpdate | 68 |
| 14.4. Patches and New Product Versions | 68 |

Remote Management 70

| | |
|---|-----|
| 15. Bitdefender Remote Admin | 71 |
| 15.1. Getting Started | 72 |
| 15.2. Status | 73 |
| 15.2.1. Services | 73 |
| 15.2.2. License | 74 |
| 15.2.3. About | 75 |
| 15.3. Policies | 76 |
| 15.3.1. Configuring Group Policies | 77 |
| 15.4. Quarantine | 87 |
| 15.4.1. Malware Quarantine | 87 |
| 15.4.2. Spam Quarantine | 89 |
| 15.4.3. Deferred Quarantine | 91 |
| 15.5. Components | 93 |
| 15.5.1. Antispam | 93 |
| 15.5.2. Spam Submissions | 94 |
| 15.5.3. SMTP | 94 |
| 15.6. Maintenance | 96 |
| 15.6.1. Bitdefender Live! Update | 96 |
| 15.6.2. Patches | 96 |
| 15.6.3. Users | 97 |
| 15.6.4. Global Proxy | 98 |
| 15.7. Reports | 99 |
| 15.7.1. Statistics | 99 |
| 15.7.2. Charts | 100 |
| 15.8. Logging | 101 |
| 15.8.1. File Logging | 101 |
| 15.8.2. Mail Alerts | 102 |
| 16. SNMP | 103 |
| 16.1. Introduction | 103 |
| 16.2. The SNMP Daemon | 103 |
| 16.3. The Bitdefender Logger Plugin | 104 |
| 16.3.1. Prerequisites | 105 |
| 16.3.2. Configuration | 105 |
| 16.3.3. Usage | 108 |
| 16.4. Troubleshooting | 108 |

Getting Help 109

| | |
|--|-----|
| 17. Support | 110 |
| 17.1. Bitdefender Support Center | 110 |
| 17.2. Asking for Assistance | 111 |
| 18. Contact Information | 112 |

| | |
|---|------------|
| 18.1. Web Addresses | 112 |
| 18.2. Local Distributors | 112 |
| 18.3. Bitdefender Offices | 113 |
| Appendices | 115 |
| A. Supported Antivirus Archives and Packs | 116 |
| B. Alert Templates | 118 |
| B.1. Variables | 118 |
| B.2. Sample Results | 120 |
| B.2.1. MailServer Alert | 120 |
| B.2.2. Sender Alert | 122 |
| B.2.3. Receiver Alert | 124 |
| B.2.4. KeyWillExpire Alert | 126 |
| B.2.5. KeyHasExpired Alert | 126 |
| C. Footer Templates | 128 |
| C.1. Variables | 128 |
| C.2. Sample Results | 129 |
| C.2.1. Clean | 130 |
| C.2.2. Ignored | 130 |
| C.2.3. Disinfected | 131 |
| Glossary | 132 |

Preface

This *Administrator's Guide* is intended for all System Administrators who have chosen Bitdefender Security for Mail Servers as security solution for their email servers. 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 Linux operating systems.

This book will describe Bitdefender Security for Mail Servers, it will guide you through the installation process, teach you how to configure it to the very detail. You will find out how to use Bitdefender Security for Mail Servers, 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 reading.

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 <code>monospaced</code> characters. |
| http://www.bitdefender.com | The URL links point to some external location, on http or ftp servers. |
| documentation@bitdefender.com | Emails are inserted in the text for contact information. |
| Chapter 4 "Package installation" (p. 14) | This is an internal link, towards some location inside the document. |
| filename | File and directories are printed using <code>monospaced</code> font. |
| ENV_VAR | Environment variables are MONOSPACED CAPITALS. |

| Appearance | Description |
|-----------------------------|---|
| <i>emphasized</i> | <i>Emphasized text</i> specially marked to call your attention. |
| "quoted text" | Provided as reference. |
| command | Inline commands are printed using strong characters. |
| # command -parameter | Command examples are printed in strong monospaced characters in a 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 | Screen output and code listings are printed in monospaced characters in a specially marked environment. |
| bdlogd(8) | It refers to a man page. |

1.2. Admonitions

Admonitions are in-text notes, graphically marked, offering additional information related to the current paragraph.



Note

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



Important

This requires your attention and it is not recommended to skip 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. Book Structure

The guide consists of the following parts:

Description. You are presented Bitdefender Security for Mail Servers, its features, the product components and the basics of the integration and the scanning mechanism.

Installation. Step by step instructions for installing Bitdefender Security for Mail Servers on a system. Starting with the prerequisites for a successful installation, you are guided through the whole installation process. Finally, the uninstall procedure is described in case you need to uninstall Bitdefender Security for Mail Servers.

Getting Started. Description of basic administration and maintenance of Bitdefender Security for Mail Servers.

Advanced Usage. You are presented the Bitdefender configuration tools, how to get run-time information, how to test antivirus efficiency, how to perform updates and how to register the product.

Remote Management. You will learn how to make the best of Bitdefender Security for Mail Servers remotely, by using several remote administration tools.

Getting Help. Where to look and where to ask for help if something goes wrong.

Appendices. The Appendices present exhaustive information about configuration, email templates and in-depth discussions over tricky parts.

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

1. FEATURES AND BENEFITS

Bitdefender Security for Mail Servers brings together proactive antivirus, antispymware, antispam, antiphishing, content filtering technologies to secure the mail traffic of companies and Service Providers. Thanks to its compatibility with most major email platforms, the solution offers your company reliable protection against newly emerging malware and attempts to steal confidential and valuable data.

1.1. Key Features

- Fast and easy deployment
- Easy integration with your current mail services
- Compatible with most major email platforms
- Proactive heuristic protection against zero-day threats
- Multiple layers of antispam filtering
- Content and attachment filtering
- Antispymware and antiphishing protection
- Intuitive program interface
- Available in both 32-bit and 64-bit versions

1.2. Key Benefits

- Email Protection against Malware
 - Fights email-borne malware by filtering and blocking messages that carry dangerous active codes.
 - Offers the possibility to filter out emails containing password protected attachments, a common way to send malware through antivirus protected MTA-s.
 - Provides the possibility of separately handling riskware (applications that pose a potential threat, but which certain user groups might still need).
- Compatibility
 - Includes dedicated agents for automatic integration with several of the most popular mail transfer agents such as Sendmail (milter), Postfix, Courier, gmail and CommuniGate Pro.
 - Fully complies with FHS (Filesystem Hierarchy Standard), operating in a completely non-intrusive manner.
 - Ensures compatibility with major Linux platforms due to its `.rpm` and `.deb` packages.


- Installed in SMTP Proxy mode, it can protect any other mail server, including those running on Windows
- Increased Business Productivity
 - Reduces mail traffic and saves network resources due to its extensive antivirus protection capabilities.
 - Improves the IT manager's productivity and prevents the loss of confidential information by filtering all mail passing through the mail server based on:
 - Content (subject line, body, sender, recipient) and attachment
 - The criteria defined for the existing user groups.
 - Provides a highly efficient multi-layered antispam protection system which:
 - Reduces mail traffic by accurately classifying messages as spam, phishing or legitimate.
 - Allows configuring antispam filter sensitivity by setting very demanding or relaxed thresholds for each user group.
 - Offers anti-phishing protection by detecting forged messages intended to trick their recipient into disclosing confidential data.
 - Provides WBL (White List/ Blacklist) support, allowing you to set a list of trusted and untrusted addresses based on which to respectively "always accept" or "always reject" mail.
- Increased Usability
 - Allows you to filter mail traffic more flexibly, leveraging antivirus, antispam, content and attachment filtering policies for different groups or users.
 - Generates detailed statistics and reports related to the solution's activity.
 - Sends customizable email notifications about its activity.
 - Allows you to remotely configure mail protection through its management tools.
 - A dedicated command line interface allows performing post-install configuration and administration tasks.
 - Can isolate dangerous or restricted mail in a quarantine zone to be dealt with later.
 - The quarantine area is searchable based upon regular expressions, sender, recipient, date and cause.
 - Allows performing management actions via SNMP by means of its SNMP Daemon Plugin.
 - Can send virus and administration alerts to three different hosts, through the SNMP Logger plugin.
 - Can send detection and other product messages to the system logger, through the SYSLOG logger plugin.


2. ARCHITECTURE

Bitdefender Security for Mail Servers is a highly complex modular structure. It is made up of several central components and additional modules, each of them having assigned a specific task. The modules are loaded during Bitdefender Security for Mail Servers startup and enabled or not, according to the user's preferences. On Linux systems, these components run as daemons, on one or multiple threads, and communicate with the others.

2.1. Core Modules

Listed by their file names, the core modules are represented in the following table.

| Module | Description |
|---|---|
| bdmond | The Bitdefender Core Monitor is the supervisor of several Bitdefender Security for Mail Servers modules. When one of them crashes, the Core Monitor isolates the object causing the crash in a special quarantine directory, notifies the administrator and restarts the involved module. Thus, even if one process dies, the whole filtering activity is not disturbed, ensuring continuous server protection. |
| bdscand | This is the Bitdefender Scan Daemon. Its purpose is to integrate the scanning engines, receive scanning requests from several daemons, such as the mail daemon or the file daemon. It scans the objects, takes the necessary actions and sends back the object and the scanning results. |
| bdmaild | The Bitdefender Mail Daemon has the role of receiving scanning requests from the MTA integration agents. It calls the Scan Daemon to perform the scan, expecting the scanning results from it. Then it applies its actions and sends back the results to the MTA integration agent. |
| bdregd | The Bitdefender Registry is made up of the bdregd program and a set of XML files, where it stores the Bitdefender Security for Mail Servers configuration. The daemon receives requests to read from and to write to the settings file, requests initiated by the other processes. |
|  | Manually editing the Registry Even if the XML files are human-readable (and writable, too), you should never try to edit them manually. Due to their high complexity, the XML |

| Module | Description |
|----------------|--|
| | files should only be modified by means of the provided configuration tools, such as the bdsafe command or the Remote Administration Console. |
| bdlogd | <p>The Bitdefender Logger is a complex component, handling all logging and notification actions of Bitdefender Security for Mail Servers. There are several types of logging, all of them realized by plugins.</p> <ul style="list-style-type: none"> • <i>file logging</i>: the data is sent to a normal log file, respecting a typical format. • <i>mail notification</i>: alerts are sent by email to the server administrator or to the sender and the recipients of an email, on special events (such as infected email found). • <i>SNMP</i>: notifications can be sent through the SNMP protocol to designated hosts. • <i>SYSLOG</i>: sends product messages to the system logger. |
| bdlived | <p>The Bitdefender Live! Update is the module responsible with updating the scanning engines and some other Bitdefender Security for Mail Servers components. The module runs continuously and periodically checks the update server. It can also be triggered manually or by the Update Pushing mechanism.</p> <p> More about Bitdefender Live! Update Bitdefender Live! Update and the update process are described in Chapter 14 “Updates” (p. 66).</p> |
| bdsnmpd | bdsnmpd accepts SNMP GET and SET messages related to Bitdefender registry keys. Thus, an authorized user is able to read and modify some of the Bitdefender configuration settings remotely. |

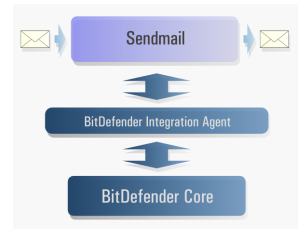
2.2. Integration Agents

Bitdefender Security for Mail Servers includes dedicated agents for automatic integration with several of the most popular mail transfer agents, such as Sendmail (milter), Postfix (generic or milter), Courier, qmail and CommuniGate Pro. Additionally, a generic SMTP Proxy agent is available for integration with virtually any mail transfer agent, including those running on Windows.

2.2.1. Sendmail

The Sendmail agent is the filtering solution for the Sendmail MTA using the Milter interface. Milter allows third-party programs to access email messages through several call-backs.

The incoming email usually arrives to Sendmail from a local or remote server. The agent calls the Bitdefender core to scan the email. After scanning, the results are passed through the same Milter interface back to Sendmail, which will deliver the message as usual, if there is something to deliver.

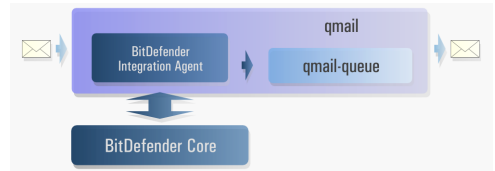


Sendmail integration

2.2.2. qmail

Inside the qmail MTA, **qmail-queue** is the central component. All the emails coming from local or remote senders pass through this component. Therefore email traffic can be captured by capturing the traffic of **qmail-queue**.

Remote or local incoming emails are first passed to the Bitdefender qmail integration agent. This will send them to the Bitdefender core for scanning and then to the original **qmail-queue**, which will deliver them as usual. From the qmail point-of-view, the filtering process is transparent.

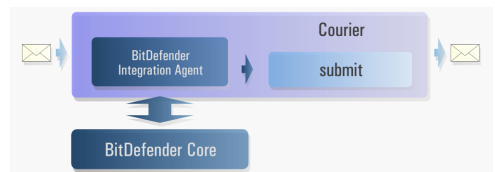


qmail integration

2.2.3. Courier

The central module of the Courier system is **submit**, an uniform mechanism which adds messages to the mail queue. Capturing its traffic is capturing the server's traffic.

Remote or local incoming emails are first passed to the Bitdefender Courier integration agent, named **bdcourier**. This will pass them on to the Bitdefender core for scanning and then to the original **submit**, which will



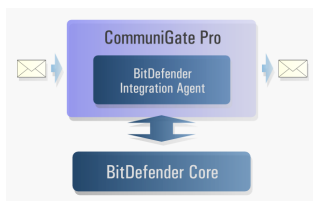
Courier integration

enqueue them as usual. From the Courier point-of-view, the filtering process is transparent.

2.2.4. CommuniGate Pro

The Bitdefender integration agent should be incorporated by the CommuniGate Pro, using its own filtering mechanism, in order to receive the email traffic.

Remote or local incoming emails are passed to the Bitdefender CommuniGate Pro agent, registered as intrinsic filter. This will call the Bitdefender core to scan the emails and then pass them back to the MTA, which will process them as usual.

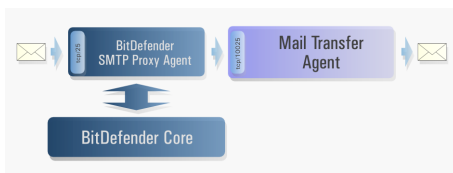


CommuniGate Pro integration

The SMTP integration varies with each other MTA.

Since we can not cover all possible variants, we can offer a short description of the integration and let you figure out how to apply it to your SMTP server.

The incoming email will arrive on port 25 of the server. On this port it is not the original Mail Transport Agent that is listening, but a special Bitdefender component, the SMTP Proxy module. On receiving the message, the Bitdefender Agent will pass it to the Bitdefender core for scanning. The core does the usual scanning and passes the results back to the agent. If found clean or if there is something to pass to the MTA, Bitdefender SMTP Proxy agent contacts the MTA on the new port this is configured to listen on, by default 10025, and sends the email, as if coming from the original source. The whole filtering process is transparent to the Mail Transport Agent.



SMTP Proxy integration

Bitdefender and MTA on different servers

Bitdefender SMTP Proxy can be installed on one server passing the scanned emails to the MTA, running on another server. In this case, the MTA can listen on the default SMTP port, 25, as usual.

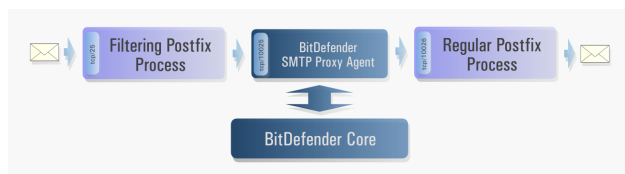
2.2.6. Postfix

For Postfix, two integration options are available: the generic SMTP proxy or the milter agent.

The generic SMTP proxy integration

The SMTP proxy integration uses external, medium-weight, real-time Content Inspection method, as described in the original Postfix documentation.

There are two Postfix processes running. The first one, listening on the standard SMTP port, receives all the incoming traffic and does the usual email filtering. The second one, listening on a higher port, by default 10026, receives the email from the filter and sends it to the standard processing.



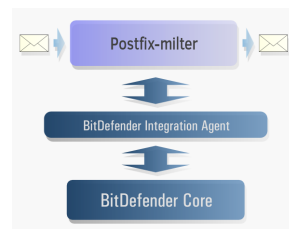
Postfix-SMTP Proxy integration

In the middle, there is the Bitdefender SMTP proxy agent listening on another higher port, 10025 by default. It receives all the traffic passed from the first process, passes it to the Bitdefender core for scanning and finally sends the traffic to the second Postfix process.

The milter agent integration

The Milter agent can also be used as a filtering solution for the Postfix MTA using the interface with the same name. Milter allows third-party programs to access email messages through several call-backs.

The incoming email usually arrives to Postfix from a local or remote server. The agent calls the core to scan the email. After scanning, the results are passed through the same Milter interface back to Postfix, which will deliver the message as usual, if there is something to deliver.



Postfix-milter integration



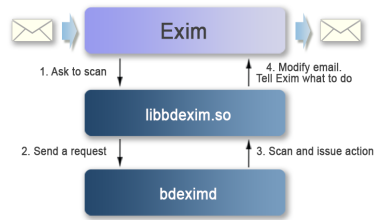
Note

For the Milter integration, Postfix 2.4.5 or later is required.

2.2.7. Exim

The Bitdefender integration leverages Exim's ACL system. It provides two components: a library, named libbdexim.so, and a daemon, named bdeximd.

When an email arrives, Exim calls libbdexim.so. The library forwards the requests to bdeximd, which scans the email. After scanning, a status is issued used to determine whether Exim should drop the email or deliver it.



Exim integration

2.2.8. Axigen

The Axigen agent uses Milter as an interface between MTA and Bitdefender Core. Milter allows third-party programs to access emails through several callbacks.

The agent calls the core to scan the email. After scanning, the results are passed back to Axigen via Milter interface, which will make the delivery if the email is safe.



INSTALLATION

3. PREREQUISITES

Bitdefender Security for Mail Servers can be installed on package-based Linux distributions (rpm or deb). The packages include all the necessary pre-install, post-install, pre-remove and post-remove scripts. The adequate package type should be installed according to the target operating system.

3.1. System Requirements

Before installing Bitdefender Security for Mail Servers, you must verify that your system meets the following system requirements:

3.1.1. Hardware Requirements

Processor

Intel® Pentium or AMD64 compatible processor, minimum 1GHz

RAM memory

Minimum: 512 MB

For improved performance, it is recommended to have at least 1 GB.

Free disk space

Minimum: 500 MB

It is recommended to have at least 1 GB, as the log and quarantine directories increase in time.

3.1.2. Software Requirements

Bitdefender Security for Mail Servers installs on Linux systems with kernel version at least 2.6.32.

Bitdefender also requires `glibc` version 2.11.3 or newer and OpenSSL 1.0.0 or newer.

Supported Linux distributions:

- Red Hat Enterprise Linux 6 or newer
- SuSE Linux Enterprise Server 11 SP3 or newer
- Debian GNU/Linux 8 (Jessie), or newer
- Ubuntu Server 14.04 LTS or newer
- CentOS 6 or newer

3.1.3. Internet Connection

Bitdefender Security for Mail Servers requires Internet access, either directly or through an HTTP proxy.

3.1.4. Mail Servers Minimum Required Versions

Sendmail

Version 8.12.1, with Milter interface

Postfix

Versions 2.x



Note

For the Milter integration, Postfix 2.4.5 or newer is required.

qmail

Version 1.03 or newer

Courier

Versions 0.42.x or newer

CommuniGate Pro

Version 4.1.1 or newer

SMTP

Any SMTP server able to listen on another port than 25.

Exim

Version 4.84.2 or newer

Axigen

Version 9.x or newer

3.2. Package Naming Convention

The installation kit is named according to the following rule:

```
Bitdefender-Security-Mail-{os}-{arch}.{pkg}.run
```

| Variable | Description |
|-------------|--------------------------------|
| <i>{os}</i> | The operating system is Linux. |

| Variable | Description |
|---------------------|--|
| <code>{arch}</code> | The architecture contains the processor class. <code>i586</code> and <code>amd64</code> are currently supported. |
| <code>{pkg}</code> | This stands for the package management tool name. Therefore, it is <code>rpm</code> for Red Hat Manager and <code>deb</code> for Debian. |

4. PACKAGE INSTALLATION

This chapter explains how to install Bitdefender Security for Mail Servers on your mail server.

i Note

For integrations with Axigen, SELinux and Zimbra solutions, refer to these KB articles:

- [How to integrate Bitdefender Security for Mail Servers with Axigen Mail Server](#)
- [How to configure SELinux when using Postfix or Sendmail militer](#)
- [Integrating Bitdefender Security for Mail Servers with Zimbra Collaboration](#)

4.1. Getting the Package

You can get the installation package from your local Bitdefender representative or download it from the Bitdefender servers.

The package comes in these flavours:

- `rpm` for distributions using the RedHat Linux package management
- `deb` for distributions using Debian Linux packaging system

4.2. Installing the Package

There is a common installation method for `rpm` and `deb`. The packages should be installed using the following command:

```
# sh Bitdefender-Security-Mail-{os}-{arch}.{pkg}.run
```

This will unpack the Bitdefender packages, according to the package type, and install them using the package manager. The packages contain the Bitdefender Security for Mail Servers files (engines, core, etc.), the install and uninstall scripts.

Example:

To install Bitdefender Security for Mail Servers on a RedHat based distribution you have to run the following command:

```
# sh Bitdefender-Security-Mail-{os}-{arch}.rpm.run
```


4.2.1. Additional Parameters

For the not-so-impatient user, the self-extractable archive provides some command line parameters, described in the following table:

| Parameter | Description |
|-------------------------------------|---|
| <code>--help</code> | Prints the short help messages. |
| <code>--info</code> | This will print the 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 packaging date. |
| <code>--list</code> | 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. |
| <code>--check</code> | <p>This is one of the most useful options, because it enables the user to verify package integrity, as stated above. The integrity is checked comparing the embedded md5 checksum (generated during packaging) with the one computed at the time of the check. If they match, the output will be the following:</p> <pre>MD5 checksums are OK. All good.</pre> <p>If not, an error message will be shown, displaying the non-matching stored and computed checksums, as follows:</p> <pre>Error in MD5 checksums: X is different from Y</pre> |
| <code>--confirm</code> | The user will be asked to confirm every step of the install process. |
| <code>--keep</code> | By default, the archive content is extracted to a temporary directory, which will be removed after the embedded installer exits. Adding this parameter to the script will not remove the directory. |
| <code>--target directory</code> | 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 |
|--------------------------|--|
| <code>--uninstall</code> | Run the embedded uninstaller script instead of the normal installer. |

4.3. Initial Setup

After unpacking the archive, the installer is launched. This is a text based installer, created to run on very different configurations.

Follow the installer prompts to complete installation and initial setup. To accept the default configuration the installer offers (which is recommended), just press the `ENTER` key when prompted.

1. License Agreement

The License Agreement is displayed. You are invited to read the full content by pressing the `SPACE` bar to go to the next page or `ENTER` for one line a time. In order to continue the installation process, you must read and agree to 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 to the License Agreement and the installation process will stop.

2. Configuring Update Notifications

You can set Bitdefender Security for Mail Servers to inform you about updates and patches. To enable this feature, type `y`, then provide the address and port of your SMTP server and the email address to send notifications to.

3. Integrating Bitdefender with the Mail Transfer Agents (MTAs)

Select the appropriate integration option.

1. CommuniGate Pro
2. Courier
3. Postfix-SMTP Proxy
4. Postfix-milter
5. qmail
6. Sendmail-milter
7. SMTP Proxy - works with any Mail Transfer Agent

For example, enter `6` to install the integration agent for Sendmail.

**Note**

Postfix-milter works only with Postfix mail server version 2.4.5 or newer. For older versions of Postfix, select Postfix-SMTP Proxy.

4. Configuring RBL Servers

You can specify a number of RBL servers in order to filter spam based on mail server's reputation as spam sender.

5. Entering Your Registration Key

Enter a registration key or press ENTER to continue with a 30 days trial.

6. Configuring Remote Administration

The remote administration is performed through a web based console. To install the console you need to provide the local IP address of the machine where Bitdefender Security for Mail Servers is installed, using the syntax `IP:port` (the default setting is `127.0.0.1:8139`). Use the generated SSL certificate to secure browser connection when accessing the console. You also need to specify the password for console authentication.

At this point, the installer has acquired all the necessary information and it will begin the install process. Basically, it will install the engines, the binaries and the documentation and it will make the post-install configuration. This is a short list of its actions on your system:

- Creates the `bitdefender` user and group and assigns the installation directory to it.
- Installs the manpages.
- Appends to the dynamic library loader configuration file the path to the Bitdefender Security for Mail Servers libraries.
- Creates a symbolic link to the configuration directory in `/etc`.
- Integrates Bitdefender Security for Mail Servers in the system init scripts.
- Finally, Bitdefender Security for Mail Servers is started-up.

5. UNINSTALL

If you ever need to remove Bitdefender Security for Mail Servers, there are several methods to do it, depending on the package type.

Note The uninstaller keeps the `/opt/BitDefender/` folder with product configuration for reinstallation purpose. When reinstalling, it is recommended to use the same package as before and then perform an upgrade, otherwise you receive a warning. Nevertheless, the product's functionality is not affected. For a complete uninstallation of Bitdefender Security for Mail Servers, you need to manually delete the `/opt/BitDefender/` folder.

5.1. Uninstalling the RPM Package

To uninstall Bitdefender Security for Mail Servers on an `rpm` package manager based distribution, you have to run the following commands:

```
# rpm -e BitDefender-radmin
# rpm -e BitDefender-mail
# rpm -e BitDefender-common
```

5.2. Uninstalling the DEB Package

To uninstall Bitdefender Security for Mail Servers using `dpkg`, on a `deb` package manager based distribution, you have to run the following commands:

```
# dpkg -r BitDefender-radmin
# dpkg -r BitDefender-mail
# dpkg -r BitDefender-common
```

5.3. Manual Uninstallation

You can also uninstall the product this way:

```
# Bitdefender-Security-Mail-{os}-{arch}.{pkg}\
  .run --uninstall
```



GETTING STARTED

6. START-UP AND SHUT-DOWN

Bitdefender Security for Mail Servers should be integrated into the system init scripts, in order to start at system initialization and stop at system shut down. Once integrated, the server will be protected all the time, since all Bitdefender services will be up and running. Normally, there is no need for the user to manually start or stop Bitdefender Security for Mail Servers, but there are administrative tasks when such actions might be necessary. In this chapter you will find how you can safely start and stop the Bitdefender services.

The **bd((8))** command

The program **bd((8))**, included in Bitdefender programs, plays the role of init script. Among the many parameters it supports, there are the standard `start`, `stop`, `restart`, with obvious actions. The standard location of the program is `/opt/Bitdefender/bin/bd`, in case of a standard straight-forward installation. If you have chosen a different installation directory, please use the correct path when calling this program.

As init script, **bd((8))** is symbolically linked, by the install program, to the system specific init directory, such as `/etc/init.d/bd` (for System V type initscripts) or `/etc/rc.d/rc.bd` (for BSD type initscripts). Therefore, according to your distribution, the following commands are identical, doing the same thing in the same way. For example, they will start Bitdefender Security for Mail Servers.

```
# /opt/Bitdefender/bin/bd start
- or -
# /etc/init.d/bd start
- or -
# /etc/rc.d/rc.bd start
- or -
# service bd start
```

For convenience, the program is always referred to in this document using the first form, but remember you can use all the forms presented above. Use the one that fits you best.

For easier use of the BitDefender related commands, you may also add `/opt/BitDefender/bin` directory to the `PATH` environment variable.

6.1. Start-up

To start Bitdefender Security for Mail Servers, you have to run the following command (for alternate forms, please see the note above).

```
# /opt/Bitdefender/bin/bd start
```

The result will be similar to the screen provided as an example below. Note that if you have more components installed, there will be more corresponding output lines.

```
* Starting bdregd ... [ ok ]
* Starting bdlogd ... [ ok ]
* Starting bdscand ... [ ok ]
* Starting bdmaild ... [ ok ]
* Starting bdlived ... [ ok ]
* Starting bdmond ... [ ok ]
* Starting bdsmtpd ... [ ok ]
```

Please wait for all the services to be started up. The script will return to the shell when all processes have been initialized. If there are any errors while initializing, they will be reported.

6.2. Shut-down

To shut down Bitdefender Security for Mail Servers, you have to run the following command (for alternate forms, please see the note above).

```
# /opt/Bitdefender/bin/bd stop
```

The output will be similar to the following screen, provided as an example. Note that if you have more components installed and running, there will be more corresponding output lines.

```
* Stopping bdsmtpd ... [ ok ]
* Stopping bdmond ... [ ok ]
* Stopping bdlived ... [ ok ]
* Stopping bdscand ... [ ok ]
* Stopping bdmaild ... [ ok ]
```

```
* Stopping bdlogd ... [ ok ]
* Stopping bdregd ... [ ok ]
```

The processes will be shut down in the reverse order of the start up. Please wait for all the services to be stopped. The script will return to the shell when there are no more running processes. If there are any errors while shutting down, they will be reported.

6.3. Restart

A simple restart of all the Bitdefender Security for Mail Servers services can be done by running the following command (for alternate forms, please see the note above).

```
# /opt/Bitdefender/bin/bd restart
```

The output is similar to those described above.

```
* Stopping bdsmtpd ... [ ok ]
* Stopping bdmnd ... [ ok ]
* Stopping bdlived ... [ ok ]
* Stopping bdscand ... [ ok ]
* Stopping bdmaild ... [ ok ]
* Stopping bdlogd ... [ ok ]
* Stopping bdregd ... [ ok ]
* Starting bdregd ... [ ok ]
* Starting bdlogd ... [ ok ]
* Starting bdscand ... [ ok ]
* Starting bdmaild ... [ ok ]
* Starting bdlived ... [ ok ]
* Starting bdmnd ... [ ok ]
* Starting bdsmtpd ... [ ok ]
```

The processes will be shut down in reverse order, then started up. Please wait for all the services to be stopped, then started. The script will return to the shell when the action is complete. If there are any errors while shutting down or starting up, they will be reported.

7. BITDEFENDER STATUS OUTPUT

Since all of its components are daemons, Bitdefender works in the background, with little or even no output at all. One source of information about the actions of Bitdefender Security for Mail Servers are the logs, if enabled. Instant real-time reports can be obtained by using the built-in facilities of status and statistical reporting.

7.1. Process Status

A short description of all running processes and their process-id (PID) is available on running the following command.

```
# /opt/Bitdefender/bin/bd status
```

Invocation of **bd((8))** command

A short discussion about different forms of invoking command **bd((8))** can be found in [Chapter 6 “Start-up and Shut-down” \(p. 20\)](#).

Output on non-NPTL systems

On non-NPTL systems, the output is slightly different. Instead on displaying only one thread, all the PIDs of all threads are shown. You should see the multiple process IDs for child threads.

7.2. Basic Information

Using the text console, more information about the current status of Bitdefender Security for Mail Servers is available when issuing the following command:

```
# /opt/Bitdefender/bin/bd info
```

Invocation of **bd((8))** command

A short discussion about different forms of invoking command **bd((8))** can be found in [Chapter 6 “Start-up and Shut-down” \(p. 20\)](#).

Bitdefender Registry

Since this information is stored inside the Bitdefender Registry, the **bdregd** daemon should be running in order to see all of it. If not, only a small part will be shown.

The following information is displayed:

- The current version of Bitdefender Security for Mail Servers along with some system information.
- The quarantine status.
- The version of installed BitDefender Core Components and Integration Agents.
- The number of signatures, the time when Bitdefender last checked for virus signatures updates and the time when it actually updated its signatures.

7.3. Statistical Report

Statistical reports about Bitdefender Security for Mail Servers activity can be obtained when running the following command:

```
# /opt/Bitdefender/bin/bd stats
```

Invocation of **bd((8))** command

A short discussion about different forms of invoking command **bd((8))** can be found in [Chapter 6 "Start-up and Shut-down" \(p. 20\)](#).

8. MTA INTEGRATION

After Bitdefender Security for Mail Servers has been installed, you have to integrate it in your Mail Transfer Agent. This means you have to redirect the email traffic through the Bitdefender integration agents, for each message to be scanned. To do so, use the `bdsafe(8)` command.

```
# bdsafe agent integrate [MTA]
```

This will automatically integrate the Bitdefender agent into your MTA installation. Then, you should consider enabling it by using the command:

```
# bdsafe agent enable [MTA]
```

These are the available MTA options:

- `cgate`
- `courier`
- `milter`
- `postfix`
- `postfix-milter`
- `qmail`
- `smtp`

8.1. CommuniGate Pro

For a manual integration of the Bitdefender agent, please follow these steps:

1. Open the CommuniGate administration interface: point your browser to the web-based management interface on the server (usually on port 8010: `http://yourserver:8010/`).
2. Go to **Settings** → **General** (you will be required to login).
3. Go to the **Helpers** tab and look at **Content Filtering**.
 - For CommuniGate Pro version 4, do the following actions:
 - a. Check the **Use Filter** box
 - b. Enter `Bitdefender` in the textbox
 - c. Set the **Log list to Problems**

- d. Set **Timeout** to 2 minutes
- e. In the **Program Path**, enter `/opt/Bitdefender/bin/bdcdgated`
- f. Set **Auto-Restart** to 5 seconds
- g. Press **Update**
- For CommuniGate Pro version 5, the method is slightly different:
 - a. Enable the filter using the drop-down combo
 - b. Enter `Bitdefender` in the corresponding textbox
 - c. Set the Log Level to **Problems**
 - d. Set **Timeout** to 2 minutes
 - e. In the **Program Path** textbox, enter `/opt/Bitdefender/bin/bdcdgated`
 - f. Set **Auto-Restart** to 5 seconds
 - g. Press **Update**
4. Go to **Settings** → **Mail** → **Rules** tab.
5. Enter `Bitdefender` and press **Create New** or **Add Rule**, in version 5.
6. Press the **Edit** button next to the **Bitdefender** filter. Do the following settings:
 - look at the **Data** list and set it to **Message Size**
 - Set **Operation** to "greater than"
 - Set **Parameter** to 1
 - Look at the **Action** list and set it to **External Filter**
 - Enter `Bitdefender` in the **Parameters** box
 - Press **Update**

Bitdefender Security for Mail Servers will now start scanning your incoming messages.
7. Restart the Bitdefender services.
8. Restart CommuniGate Pro.

9. BASIC CONFIGURATION

9.1. View Settings

After you have installed the Bitdefender Security for Mail Servers, it may be a good idea to understand how security policies work.

The first thing to remember is that security policies apply to groups.

By default you are dealing with one group only, referred to as `Default`, which contains the entire list of users, both senders and receivers, and specifies the implied settings, if they are not otherwise specified in a certain group.

Note
Older installations, using packages prior version 3.1.0, have two groups: `All` and `Default`. On versions 3.1.0 or higher, `All` has been replaced by `Default`.

Note
For detailed information about adding and editing groups, see [Section 11.1.1 “Adding and Editing Groups”](#) (p. 36) and, of course, the `bdsafe(8)` manual pages.

Naturally, the second thing to do is to have a look at the default security settings. Run this command as root.

```
# bdsafe group configure Default
```

The output will be similar with the one below.

```
Configuration for 'addfooters', group 'default':  
addfooters = 'Y'
```

```
Configuration for 'smtpforward', group 'default':  
enable      = 'N'  
when        = 'BeforeScan'  
smtpphelo   = ''  
smtpfrom    = ''  
smtpprcpt   = ''  
smtpip      = '127.0.0.1'  
smtpport    = ''
```

```
Configuration for 'antivirus', group 'default':
```

```
enable                = 'Y'  
addheaders            = 'Y'  
headername            = 'X-BitDefender-Scanner'  
actionsonriskware     = 'disinfect;delete;quarantine'  
actionsonsuspected    = 'disinfect;delete;quarantine'  
actionsonvirus        = 'disinfect;delete;quarantine'  
actionsonpassword     = 'ignore'  
pipeprogram           = ''  
pipeprogramarguments = ''
```

```
Configuration for 'antispam', group 'default':
```

```
enable                = 'Y'  
addheaders            = 'Y'  
cgatecompat           = 'N'  
modifysubject         = 'Y'  
aggressivity          = 'default'  
actions               = 'ignore'  
whitelist              = '/opt/BitDefender/etc/as_Default_whitelist'  
blacklist              = '/opt/BitDefender/etc/as_Default_blacklist'  
headername            = 'X-BitDefender-Spam'  
stampheadername       = 'X-BitDefender-SpamStamp'  
headertemplateham     = '/opt/BitDefender/share/templates/ham.tpl'  
headertemplatespam   = '/opt/BitDefender/share/templates/spam.tpl'  
subjecttemplate       = '/opt/BitDefender/share/templates/subject.tpl'  
usebwfilter           = 'Y'  
usebayesfilter        = 'Y'  
usemultifilter        = 'Y'  
userblfilter          = 'N'  
useurlfilter          = 'Y'  
usesignfilter         = 'Y'  
usesurblfilter        = 'Y'  
useiprblfilter        = 'Y'  
useapmfilter          = 'Y'  
usecloud              = 'Y'  
markinfected          = 'N'  
pipeprogram           = ''  
pipeprogramarguments = ''
```

```
Configuration for 'contentfilter', group 'default':
```

```
enable                = 'Y'  
rules                 = ''
```

```

maxrules      = ''
headername    = 'X-BitDefender-CF-Stamp'
htmldisarm    = 'N'
multimatch    = 'N'

```

Each setting will be explained in the following table.

| Setting | Value |
|-----------------------------|---|
| AddFooters | Y if it is enabled, N if it is disabled. Add a new footer to all mails or not. |
| SmtplibForward/Enable | Y if you forward mails to another mail server, N if SmtplibForward is disabled. |
| SmtplibForward/When | Shows if the mail messages are to be forward to another mail server before or after scanning. |
| SmtplibForward/SMTP_HELO | Shows the other mail server HELO protocol command. |
| SmtplibForward/SMTP_FROM | Shows the other mail server MAIL FROM protocol command. |
| SmtplibForward/SMTP_RCPT_TO | Shows the other mail server RCPT TO protocol command. |
| SmtplibForward/SMTP_IP | Shows the other mail server IP address. |
| SmtplibForward/SMTP_PORT | Shows the other mail server port. |
| Antivirus/Enable | Y if the antivirus module is enabled, N if it is disabled. |
| Antivirus/AddHeaders | Y if it is enabled, N if it is disabled. Add a new header to all mails or not. |
| Antivirus/HeaderName | Shows the default antivirus header. |
| Antivirus/ActionsOnRiskware | Lists the actions to be taken when riskware message is found. |

| Setting | Value |
|--------------------------------|--|
| Antivirus/ActionsOnSuspected | Lists the actions to be taken when suspected message is found. |
| Antivirus/ActionsOnVirus | Lists the actions to be taken when virus infected message is found. |
| Antivirus/PipeProgram | Shows the full path to the program to pipe the mail to. |
| Antivirus/PipeProgramArguments | Shows the corresponding argument the pipe program accepts. |
| Antispam/Enable | Y if the antispam module is enabled, N if the antispam module disabled. |
| Antispam/AddHeaders | Y if it is enabled, N if it is disabled. Add a new header to all mails or not. |
| Antispam/ModifySubject | Y if it is enabled, N if it is disabled. Specifies whether the subject of the email message should be modified conforming to the <code>Subject</code> template field or not. |
| Antispam/Aggressivity | Sets up the antispam <code>Aggressivity</code> level. It goes from 0 (minimum trust in antispam score returned by the Bitdefender filters) up to 9 (maximum trust). |
| Antispam/Actions | Lists the actions to be taken when spam message is found. |
| Antispam/WhiteList | Shows the path to the white list configuration file. |
| Antispam/BlackList | Shows the path to the black list configuration file. |
| Antispam/StampHeaderName | Shows the default spam header. |
| Antispam/HeaderTemplateHam | Shows the path to the ham header template file. |

| Setting | Value |
|---------------------------------|--|
| Antispam/HeaderTemplateSpam | Shows the path to the spam header template file. |
| Antispam/SubjectTemplate | Shows the path to the subject template file. |
| Antispam/Engines/UseBWFilter | Y if the antispam Black/White list filter is enabled, N if it is disabled. |
| Antispam/Engines/UseBayesFilter | The Bayesian filter is no longer supported and will be removed from product configuration in future updates. |
| Antispam/Engines/UseMultiFilter | Y if the antispam multi-filter is enabled, N if it is disabled. |
| Antispam/Engines/UseRblFilter | Y if the antispam RBL (Real-time Blackhole List) filter is enabled, N if it is disabled. |
| Antispam/Engines/UseURLFilter | Y if the antispam URL filter is enabled, N if it is disabled. |
| Antispam/Engines/UseSignFilter | Y if the antispam signatures filter is enabled, N if it is disabled. |
| Antispam/Engines/UseSURblFilter | Y if the antispam SURBL filter is enabled, N if it is disabled. |
| Antispam/Engines/UseApmFilter | Y if the antispam advanced pattern matching filter is enabled, N if it is disabled. |
| Antispam/Engines/UseCloud | Y if the antispam engines should query the cloud for improved detection, N if it should not. |
| Antispam/PipeProgram | Shows the full path to the program to pipe the mail to. |

| Setting | Value |
|-------------------------------|--|
| Antispam/PipeProgramArguments | Shows the corresponding argument the pipe program accepts. |
| ContentFilter/Enable | Y if the content filtering is enabled, N if it is disabled. |
| ContentFilter/Rules | Shows the location of the content filter configuration file. |
| ContentFilter/MaxRules | Shows the maximum number of rules that can be loaded from the content filter configuration file. |
| ContentFilter/Administrator | Shows the user to be notified about block or allow emails based on analysis of their content. |
| ContentFilter/SMTPServer | Shows the hostname and port in case you want to forward mails based on analysis of their content to another mail server. |

The default security settings apply to the `Default` group and to any newly created group.

9.2. Edit Settings

You can customize a certain group to meet your needs, by changing its settings. In this way, the new settings will have higher precedence over the default ones. For example, let's suppose you want to add a group named `Secretary`. Run these commands as root.

```
# bdsafe group insert Secretary \  
    recipient:my_secretary@example.com
```

```
# bdsafe group priority Secretary 4
```

**Note**

The group priority will be 4. To understand what group priority is all about, please see the [Section 11.1.3 “Group Priority”](#) (p. 39).

And you want that your secretary never misses a mail, even if it looks like spam. The **bdsafe** command for ignoring spam for the `Secretary` group is the following.

```
# bdsafe group configure Secretary \  
  antispam actions ignore
```

Maybe you want to enable the Asian characters filter in order to cut down the amount of spam originating from Far East.

```
# bdsafe mail antispam charsets \  
  asian enable
```

To check the configuration status of the mail daemon component, run this command.

```
# bdsafe mail
```

**Note**

For a full description of Bitdefender Security for Mail Servers settings you must take a look at the `bdsafe(8)` manual pages.

10. 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 product, you have to provide a new license key.

To check the license status, use the following command.

```
# bdsafe license mail
```

You will be presented with the license type, status, the number of covered users and the remaining validity period.

If you have a new license key, the following command will perform the registration of the installed daemon.

```
# bdsafe license mail ABCDE12345ABCDE12345
```



Important

Internet access is required for license activation and periodic validation.



ADVANCED USAGE

11. CONFIGURATION

Once Bitdefender Security for Mail Servers has been installed and integrated into the Mail Transport Agent, it just works. But there are some settings to fine-tune your installation that you might be interested in.

11.1. Group Management

The Bitdefender Group Management component is used to manage users and settings as groups in a very flexible way. It can be easily integrated with any application requiring this feature. We will present you just some introductory commands. For detailed information, please see the `bdsafe(8)` manual pages.

11.1.1. Adding and Editing Groups

The users are defined according to their email address, as they are seen by the server internally. Several users define a group. The nice part is that you can specify various settings for each group, such as antivirus actions, templates to be used for notification and so on.

We shall create a new group, add some users and apply some settings.

First, create a group and add a user identified by his email address: `user1@domain.com`. Later we can add some more. Open a terminal and run the following as root.

```
# bdsafe group insert GROUP_NAME sender:user1@domain.com
```

We should clarify some things, before proceeding to the next step. The `bdsafe` command is the main Bitdefender configuration tool. It would be wise to have a look at the `bdsafe(8)` manual page, to get an idea about its options and usage.

Note

When specifying email addresses, you can use the following wildcards to define an entire email domain or a pattern for email addresses:

- Asterisk (*), replacing zero, one or more characters.
- Question mark (?), replacing any single character.

Second, the `sender` option will identify the users only as email senders. If you need to identify them as receivers, change it to `recipients`.

At this moment, we can list the groups and the users to check whether the previous command worked. Here is the command you should run.

```
# bdsafe group list GROUP_NAME
```

Let's add a recipient user.

```
# bdsafe group insert GROUP_NAME recipient:user2@example.com
```

Now, we have a group and some users inside the group. Let's change the antivirus actions to `disinfect;quarantine`. We have to use the same `bdsafe(8)` command. Note the method used for the string to escape the shell.

```
# bdsafe group configure GROUP_NAME antivirus \  
  actionsonvirus 'disinfect;quarantine'
```

Or maybe you want to alter the spam threshold for the same group.

```
# bdsafe group configure GROUP_NAME antispam aggressivity 9
```

Let's use the `Default` group, too. By default, the email footers are appended. Here is the command to disable them:

```
# bdsafe group configure Default addfooters N
```



Note

The footers cannot be disabled if the product is registered with a trial key.

Next, you can use the mail forward feature, enabling message sending to another recipient. In order to do this, run this command as root:

```
# bdsafe group configure GROUP_NAME \  
  smtpforward smtpip [IP_ADDRESS]
```

Eventually, you will want to remove the group.

```
# bdsafe group remove GROUP_NAME
```

11.1.2. Integration with an LDAP Server

The process of creating groups can be easily simplified when you integrate the Bitdefender Security for Mail Servers with an LDAP (Lightweight Directory Access Protocol) server. The **bdsafe** command can be used to access and import groups and users from the LDAP server.

To access the respective LDAP server you must follow these steps:

```
1. # bdsafe ldap configure server \  
    "ldap://example.test.ro:8000"
```

This command will set the address of the respective LDAP server. The `url` argument must follow the syntax: `ldap://server:port`.

```
2. # bdsafe ldap configure basedn \  
    "ou=Test,ou=Test Team,dc=example1,dc=example2"
```

This command will set the top level of the LDAP directory tree. The replaceable argument represents the distinguished name of the LDAP entry (see RFC 1779 - A String Representation of Distinguished Names for more details).

```
3. # bdsafe ldap configure user "test\example1"
```

This command is used to set the LDAP username.

For the Active Directory servers, the user can also have the `domain\user` syntax. Either quote user names or just escape the backslash.

```
4. # bdsafe ldap configure passwd set
```

This command is used to set the LDAP password. After running it, just type the password.

To import a group from the respective LDAP server you must follow these steps:

```
1. # bdsafe ldap group list
```


This command is used to display all LDAP groups.

2.

```
# bdsafe ldap group list GROUP_NAME
```

The users of the specified group will be displayed.

3.

```
# bdsafe ldap group import GROUP_NAME "senders"
```

The command is used to automatically add a group identical with the one from the LDAP server. In the above-mentioned examples, the group members are added as senders. Of course, they can also be added as recipients.


11.1.3. Group Priority

The group priority attribute, when properly used, can be a very useful instrument. At the same time, if it remains not completely understood can cause some issues.

Let's take a simple example. Suppose you have created 7 groups: `Marketing`, `HR`, `Secretary`, `Admin`, `Technical`, `Finance`, `Dangerous`. Besides those groups, remember you are already dealing with the `Default` group (or `All` for old installations), containing the entire list of users.

For every group you configured some customised settings: let's say a relaxed antispam policy for the `Secretary`, `Admin` and `Marketing` groups, and a more aggressive one for the `HR`, `Finance` and `Technical` groups. Furthermore, you needed a collection of viruses and spam messages for your security tests, and set Bitdefender Security for Mail Servers to ignore malware and illicit messages for the `Dangerous` group.

Each group has a specified priority. For example, the `Secretary` group has priority 4.

 **Note** Remember that the `Default` group has the priority set to 1 (the highest priority).

For the sake of discussion, let's suppose that the group priority situation is the following.

| Group | Priority |
|---------|----------|
| Default | 1 |

| Group | Priority |
|-----------|----------|
| Dangerous | 2 |
| Marketing | 3 |
| Secretary | 4 |
| Admin | 5 |
| HR | 6 |
| Technical | 7 |
| Finance | 8 |

In this case, the first security policy to be applied is that corresponding to the `Default` group, let's say one that disinfects viruses and deletes spam messages. The second one to be applied is the policy corresponding to the `Dangerous` group and so on.

So, what do you think of your spam messages and virus infected files collection? You will get almost nothing, because the `Default` group policy applies first.

To change this situation, you have to set the `1` priority for the `Dangerous` group. To do this, run this command as root:

```
# bdsafe group priority Dangerous 1
```

The group priority order will be now the following one.

| Group | Priority |
|-----------|----------|
| Dangerous | 1 |
| Default | 2 |
| Marketing | 3 |
| Secretary | 4 |
| Admin | 5 |
| HR | 6 |

| Group | Priority |
|-----------|----------|
| Technical | 7 |
| Finance | 8 |

Naturally, a good idea would be to change the `Default` group priority to 8, to not compromise the other security policies. Run this command as root.

```
# bdsafe group priority Default 8
```

The group priority order will be now the following one.

| Group | Priority |
|-----------|----------|
| Dangerous | 1 |
| Marketing | 2 |
| Secretary | 3 |
| Admin | 4 |
| HR | 5 |
| Technical | 6 |
| Finance | 7 |
| All | 8 |

Please notice that it makes sense that the `Marketing`, `Secretary` and `Admin` groups, with a relaxed antispam security policy, to have precedence over the `HR`, `Technical` and `Finance` groups, with a more aggressive one.



More from the manual pages

As stated before, these are just simple examples. Please see the `bdsafe(8)` manual pages for detailed information.

11.2. Antivirus Settings

Bitdefender antivirus engines detects not only viruses, but also other potentially malicious applications like riskware (programs that might be executed or misused

by other malware) and suspected files (containing possible malware; these are usually submitted to the AV Lab for further analysis).

You can customize your antimalware settings. By using **bdsafe** command, you can choose the actions to be performed on every type of malware.

- `actionsonvirus`
- `actionsonriskware`
- `actionsonsuspected`

For example, if you want to delete (or move to quarantine, whenever removing is not possible) every suspected object found, run this line as root.

```
# bdsafe group configure GROUP_NAME \  
  antivirus actionsonsuspected "delete;move-to-quarantine"
```



Actions order

Not all actions in every order are available. For instance, you cannot set the first action to be Delete and the second one to be Disinfect: it doesn't make sense!

Now, let's have a look at the entire list of possible actions.

Disinfect

To remove the malware from the infected attachment (or any other mail component that can be used to send malware). If successful, the mail is passed to the next plugin (if any) or forwarded. Otherwise, the next action is executed.

Delete

To remove the attachment or other mail component that contains the malware. If successful, the mail is passed to the next plugin (if any) or forwarded. Otherwise, the next action is executed.

When the mail is completely deleted, a replacement letting the recipient know what happened will be generated.

Move-to-quarantine

To move the mail to quarantine. If the action fails, an error message line is written to the log.

After this action is taken, the mail will either be dropped (the default action) or rejected.

Copy-to-quarantine

To copy the mail to quarantine. If the action fails, an error message line is written to the log.

Drop (the default action)

To send the message to the mail transport agent (MTA) to drop the mail. This is the default action. Thus, the final action will always be **Drop**, unless you decide otherwise.

This action prohibits the mail from passing. The MTA will return no response to the sender.

Reject

To send the message to the mail transport agent (MTA) to reject the mail.

This action prohibits the mail from passing. However, the MTA will send back a rejection message.

Ignore

To send the message to the mail transport agent (MTA) to forward the mail.

Pipe to program

To pipe the mail to a given program.



Using the command line

All these actions can also be configured by using the **bdsafe** tool. For a full description of these settings you must take a look to the **bdsafe(8)** manual pages.

For instance, to pipe all riskwares to the **submit.sh** program, run this command as root.

```
# bdsafe group configure GROUP_NAME antivirus \  
  actionsonriskware pipe
```

```
# bdsafe group configure GROUP_NAME antivirus \  
  pipeprogram /usr/local/bin/submit.sh
```

11.3. Antispam Settings

Bitdefender Antispam employs remarkable technological innovations and industry standard antispam filters to weed out spam before it reaches the user's Inbox.

In our field, performance means high detection rates and very few “false positives” (legitimate messages detected as spam). To achieve this goal we have packed together powerful antispam filters. These are the antispam filters, in the pass-through order.

The Multipurpose filter

The Multipurpose filter is a generic name for GTUBE (an antispam test) and two specialized filters: the Charset filter and the Sexually explicit filter.

GTUBE, the Generic Test for Unsolicited Bulk Email, is an antispam test similar to EICAR antivirus test. The test consists in entering a special 68-byte string in the message body of an email in order to be detected as spam. Its role is to check the product functionality to see if the filters are correctly installed and detect the incoming spam.

The Charset filter can be instructed to detect messages written in other languages (for instance Asian languages, or Cyrillic) and mark them as spam. This comes in handy when the user is certain that they will not receive mail in these languages.

The American law demands that all sexually explicit advertisement emails be marked as such, with “sexually explicit” in their subject. The Sexually explicit filter can detect and mark these messages as spam directly.



Note

The GTUBE is the first filter to come to action, while the specialized filters follow after the black list / white list filter.

The Black list / White list filter

The black list / white list filter can be very useful when the user wants to block incoming messages from a certain sender (blacklist), or when the user wants to make sure that all messages from a friend or a newsletter arrive in the Inbox, regardless of their contents. The black list / white list filter is often called “Friends / Spammers list”. It can define *allow* or *deny* lists both for individual email addresses, or for entire domain names (for instance all mail from any employee of bigcorporation.com).



Add friends to the white list

We recommend that you add your friends names and email addresses to the white list. Bitdefender will not block messages from those on the list; therefore, adding them ensures that legitimate messages get through.

The two lists are plain text files, containing one entry per line. You can find these text files (`as_wlist` and `as_blist`) in this location: `/opt/BitDefender/etc`. The entries may be usual email addresses or domain names, respecting the following format.

| Format | Description |
|------------------------------|---|
| <code>user@domain.com</code> | This format will match only the specified user from the specified domain. |
| <code>user@domain.*</code> | The mentioned user from any domain whose name starts with the specified text will match. |
| <code>user@*.com</code> | The user from any domain with a <code>.com</code> suffix (for example) will match. |
| <code>*@domain.com</code> | This will match all users from the specified domain. |
| <code>*@domain.*</code> | All users from all domains starting with the mentioned text will match. |
| <code>*.com</code> | This will match all users from all domains with a <code>.com</code> suffix (for example). |
| <code>user@*</code> | The specified user, from all domains, will match. |
| <code>user*</code> | This will match all users whose names start with the mentioned text, no matter of the domain. |



Important

The changes are not effective until you restart Bitdefender Security for Mail Servers

The RBL filter

RBL stands for “Real time Black List” or “Real time Blackhole List”. The Bitdefender implementation uses the DNSBL protocol and RBL servers to filter spam based on mail server’s reputation as spam sender.

The mail server address is extracted from the email header and checked for validity. If the address belongs to a private class (`10.0.0.0/8` or `192.168.0.0/16`) or it is not relevant, it will be ignored.

A DNS check will be performed on the domain `d.c.b.a.rbl.example.com`, where `d.c.b.a` is the reversed IP address of the server and `rbl.example.com`

is the RBL server. If the DNS replies that domain is valid, it means that the IP is listed in the RBL server and a certain server score is provided. This score can take values from 0 to 100, according to the server confidence (trust level), which you are free to configure.

The query is performed for every RBL server in the list and the score returned by each one is added to the intermediate score. When reaching 100, no more queries are performed.

Finally, a spam score is computed from the RBL servers score and added to the global email's spam score.

You can easily configure the RBL nameservers for the Mail daemon, by running this command.

```
# bdsafe mail antispa m rbl nameservers [add|remove] [host]
```

You can also configure the RBL servers for the Mail daemon, by running this command.

```
# bdsafe mail antispa m rbl servers [add|remove] \  
host:[weight]
```

The value of the `weight` parameter can be between 0 (minimum trust level) and 100 (maximum trust level).

The IP RBL filter also enables checking the SMTP connection IP address against the configured RBL servers. Please note that this only works for SMTP Proxy mode.

The URL filter

Almost all spam links to a site: whether they want us to buy cheap Rolexes or enter our login and password on a fake Citibank site, they have a link. The URL filter detects these links and looks them up in a database created and maintained (via update) by our lab. If a message links to a “forbidden” site, the odds are high that it's spam.

The Bayesian filter

The Bayesian filter is no longer supported and will be removed from product configuration in future updates.

The Advanced Pattern Matching (APM) - NeuNet™ filter

Based on artificial neural networks, APM is a powerful heuristic antispam filter, developed by Bitdefender to detect new and unknown spam. The APM filter is automatically trained on large volumes of spam messages inside the Bitdefender Antispam Lab. During training, it learns to distinguish between spam and legitimate emails and to recognize new spam by perceiving its similarities, often very subtle, with the messages it has already examined. This filter is designed to improve signature-based detection, while keeping the number of false positives very low.

The Cloud filter

This filter provides protection against 0-day and advanced threats based on the Global Protective Network security cloud.

Bitdefender maintains a constantly evolving database of spam mail "fingerprints" in the cloud. A query containing the email fingerprint is sent to the servers in the cloud to verify on the fly if the email is spam. Even if the fingerprint is not found in the database, it is checked against other recent queries and, provided certain conditions are met, the email is marked as spam.

For improved cloud-based detection of 0-day spam, you can use the Delayed Delivery feature (disabled by default). If a message is not detected as spam at the moment of arrival, it is placed in a queue and re-scanned after a time interval. This increases the chances that an initially undetected spam message is labeled appropriately the second time around. On the downside, email delivery will be delayed and you may notice an increase in resource consumption.

To enable Delayed Delivery, run the following command:

```
# bdsafe mail delayeddelivery enable y
```

Once you install Bitdefender Security for Mail Servers all these antispam filters are enabled. Of course, you can set up your desired number of active filters, by using the **bdsafe** command. For example, to enable / disable the URL filter, run the following command as root.

```
# bdsafe group configure \  
GROUP_NAME antispam useurlfilter [value]
```

 **Note**

The new value might be `Y`, to enable the filter, or `N`, to disable it.

For a full description of these antispam settings you must take a look to the **bdsafe(8)** manual pages.

11.3.1. X-Junk-Score Header for CommuniGate Pro Integration

When integrated with CommuniGate Pro, Bitdefender can add the X-Junk-Score header to filtered emails. CommuniGate Pro uses the value of the X-Junk-Score header to perform certain actions on the processed emails.

 **Note**

For more information about the X-Junk-Score header, please refer to the CommuniGate Pro documentation.

To enable the X-Junk-Score header, run the following command:

```
# bdsafe group configure GROUP_NAME antispam cgatecompat Y
```

To apply the configuration changes, run the following command:

```
# bdsafe reloadsettings
```

11.4. Content Filtering

Sometimes you just need to block or allow emails based on analysis of their content, rather than other criteria. Bitdefender offers support for this kind of operation.

To create, modify or delete content filtering rules you have to run one of the following **bdsafe** commands.

```
# bdsafe group configure GROUP_NAME contentfilter add \  
  {priority} {name} {type} {header_name} \  
  {condition} {value} {action} {notify}
```

| Argument | Value |
|-----------|---|
| type | header, body, attachment-name, attachment-type, attachment-size, mailsize |
| condition | exists, !exists, match, !match, greater-than, !greater-than |
| value | a positive number (of bytes), a regular expression |
| action | ignore, drop, reject, replace, copy-to-quarantine, move-to-quarantine |
| notify | none, administrator, admin, sender, recipients |

The command above adds a new content filter rule.

```
# bdsafe group configure GROUP_NAME contentfilter modify \  
  {rule_priority_number} {field_name=field_value}
```

| Argument | Value |
|------------|--|
| field_name | priority, enabled, name, type, header_name, condition, value, action, notify |

The command above modifies a rule, field by field.

```
# bdsafe group configure GROUP_NAME contentfilter dump \  
  {rule_priority_number}
```

The command above lists all existing rules for the specified group. If you add a number as argument the rule with that priority number will be displayed only.

```
# bdsafe group configure GROUP_NAME contentfilter delete \  
  {rule_priority_number}
```

The command above deletes the rule with the specified priority number.

```
# bdsafe group configure GROUP_NAME contentfilter enable \  
  {boolean_value} {rule_priority_number}
```

The command above enables/disables content filtering for a certain group. If you add a number as argument the rule with that priority number will be enabled/disabled only.

```
# bdsafe group configure GROUP_NAME contentfilter priority \  
  {old_priority_number} {new_priority_number}
```

The command above changes the priority of a certain rule.

```
# bdsafe group configure GROUP_NAME contentfilter rules \  
  {path_to_file}
```

The command above lists the group content filter configuration file location. If you add a `path_to_file` argument, this command sets the group content filter configuration file to the specified location.

```
# bdsafe group configure GROUP_NAME contentfilter maxrules \  
  {number}
```

The command above sets the maximum number of rules that can be loaded from the group content filter configuration file.

```
# bdsafe group configure GROUP_NAME \  
  contentfilter htmldisarm Y
```

The command above enables the HTML disarm feature for the specified group. This feature is designed to remove potentially malicious code like JavaScript or Visual Basic from emails with HTML content.

11.4.1. Examples

Let's take some examples to illustrate the power content filtering offers.

1.

```
# bdsafe group configure GROUP_NAME \  
  contentfilter add 0 MyRule header "Subject" "match" \  
  "porn" "drop" "none"
```

This will add the content filter rule, named `MyRule` with 0 priority (the most important) to the specified group. The rule says: when the word `porn` is found within the Subject part of the header, the respective mail will be dropped and nobody will be notified.

```
2. # bdsafe group configure GROUP_NAME \
    contentfilter add 1 Salary body "match" \
    "salar.*" "drop" "admin"
```

This will add the content filter rule, named `Salary` with 1 priority to the specified group. When applied, this rule means that emails containing in their body words like `salary`, `salaries`, `salarry`, `salariess`, `salariu` will be dropped and the administrator will be notified.

The lesson to be learn is this: if it is a must that emails containing sensitive information (like salary data, personal salary reports) to be filtered accordingly, just set a rule for them. A good idea would be to use regular expressions. The table below will provide you with some examples.

| Example | Description |
|-----------------------------------|---|
| <code>Honou?r</code> | You could use this to match either <code>Honor</code> or <code>Honour</code> . The question mark makes the preceding token in the regular expression optional. |
| <code>Dr[iaun]k</code> | You could use this to match either <code>Drink</code> or <code>Drank</code> or <code>Drunk</code> . By using this kind of regular expression (character class) one out of several characters will be matched only. |
| <code>[0-9]\sMAR\s200[5-8]</code> | You could use this to match <code>5 MAR 2005</code> or <code>3 MAR 2008</code> or <code>9 MAR 2007</code> and so on. By using a hyphen inside a character class one out of a specified range of characters will be matched only. The <code>\s</code> sign will match a space. |

| Example | Description |
|--|---|
| <code>Is+ues*</code> | You could use this to match <code>Issue</code> or <code>Issue</code> or <code>Issues</code> or <code>Issssuess</code> and so on. The <code>+</code> sign will match one or more times the preceding token. The <code>*</code> sign will match zero or more times the preceding token. |
| <code>^[0-9]+EUR</code> | You could use this to match <code>30 EUR</code> or <code>35EUR</code> or <code>023213 EUR</code> or any string starting with a digit, followed by <code>EUR</code> string. The <code>^</code> sign represents the start of the string to be matched. |
| <code>[^\s]*@example.com</code> | You could use this to match <code>noreply@example.com</code> or <code>news@example.com</code> or <code>blabla@example.com</code> and so on. The <code>^</code> sign inside brackets matches any character that is not the following token. In the above-mentioned example, <code>[^\s]*</code> will match any non-whitespace character. |
| <code>^List-I[dD]:\s.*example.com</code> | You could use this to match <code>List-Id: aNYstring example.com</code> or <code>List-ID: example.com</code> and so on. The <code>^</code> sign represents the start of the string to be matched. The <code>\s</code> sign will match a space. The <code>[dD]</code> expression means either <code>d</code> or <code>D</code> will be matched. The <code>.*</code> expression means any sign will be matched. |

**Note**

Do not to forget to escape with a backslash the metacharacters (the square or round brackets, the backslash, the caret, the dollar sign, the period, the vertical bar symbol, the question mark, the asterisk, the plus sign).

3.

```
# bdsafe group configure GROUP_NAME \  
contentfilter add 2 BigMail attachment-size \  
"greater-than" "10000" "drop" "none"
```

This will add the content filter rule, named `BigMail` with 2 priority to the specified group. When applied, this rule means that if the size of a certain attachment is greater than 10000 bytes, the email containing the respective attachment will be dropped and nobody will be notified.

4.

```
# bdsafe group configure GROUP_NAME \  
contentfilter add 3 Executable attachment-type \  
"match" "application/octet-stream" \  
"move-to-quarantine" "admin"
```

This will add the content filter rule named `Executable`, with priority 3, to the specified group. When applied, this rule will quarantine any email containing attachments with the MIME type `application/octet-stream` and notify the administrator about it.

5.

```
# bdsafe group configure Default \  
contentfilter add 0 BlockedExt attachment-name \  
"match" "[^\s]*\.(exe|scr|bat|com)" \  
"replace" "none"
```

This will add the content filter rule named `BlockedExt`, with priority 0, to the `Default` group. When applied, this rule will replace the email attachments having the specified extensions with a notification text to inform recipients about the action. No notification will be sent to administrators about this event.

6.

```
# bdsafe group configure GROUP_NAME \  
contentfilter modify 0 "priority=3" \  
"name=explicit content"
```

This will change the `MyRule` (0 priority) from the old priority 0 to new priority 3. The new name of this rule will be "explicit content".

```
7. # bdsafe group configure GROUP_NAME \  
    contentfilter priority 1 0
```

This will change the `Salary` rule of the specified group from old priority 1 to new priority 0 (the most important rule; it will be applied first of all).

```
8. # bdsafe group configure GROUP_NAME \  
    contentfilter dump
```

This will list the content filter rules of the specified group together with their priorities.

```
9. # bdsafe group configure GROUP_NAME \  
    contentfilter delete 4
```

This will delete the content filter rule of the specified group with priority 4.

```
10. # bdsafe group configure GROUP_NAME \  
    contentfilter enable N 4
```

This will disable the content filter rule of the specified group with priority 4.

11.5. The Bitdefender Logger Daemon

The Bitdefender Logger Daemon (**bdlogd**) allows you to get a full picture of the others demons activity, as it receives logging messages from the other modules and passes them to the logger plugins.

Either a local socket (Unix domain socket) or a TCP/IP socket will be used to implement communication among different modules of Bitdefender Security for Mail Servers while the communication among the Logger Daemon and its plugins is based on API (Application Programming Interface).

bdlogd was designed with a plugins parallel execution philosophy in mind. In short, this means that each plugin will run on its own individual thread. The result is that the slower plugins will no longer disturb the faster ones (like filelog).

To manage the configuration of the Logger Daemon and the associated plugins you will use the **bdsafe** command. You will be provided below with a list of common settings for **bdlogd**.

The general syntax for the **bdlogd** daemon and plugins configuration is the following one:

```
# bdsafe logger configuration [parameters ...]
# bdsafe logger plugin configuration [parameters ...]
```

The BasePath

To specify the fully-qualified name of a directory from which **bdlogd** will attempt to load plugins, run the following line as root:

```
# bdsafe logger basepath [value]
```

11.5.1. The Logger Plugins

The Bitdefender Logger Daemon supports the following plugins:

- The Filelog Plugin
- The SMTP Plugin
- The SNMP Plugin
- The SYSLOG logger Plugin

The Filelog Plugin

The **bdlogd** receives messages from the other modules and send them to the other plugins, for instance the filelog plugin. By default, the filelog plugin settings are the following:

- **bdlived.info**=/opt/Bitdefender/var/log/update.log
- **bdmaild.info**=/opt/Bitdefender/var/log/mail.log
- ***.error**=/opt/Bitdefender/var/log/error.log
- **bdlived.error**=/opt/Bitdefender/var/log/update.log
- ***.license**=/opt/Bitdefender/var/log/license.log
- **bdmaild.virus**=/opt/Bitdefender/var/log/virus.log
- **bdmaild.spam**=/opt/Bitdefender/var/log/spam.log

It means that, for example, all error-related information, coming from all Bitdefender daemons, will be found in this location:

```
/opt/Bitdefender/var/log/error.log.
```

However, you can fully customize the daemon and message type and also the file paths where the file logger writes the messages, by using the **bdsafe** command. In order to do this, please run the following line as root:

```
# bdsafe logger file path message_type [value]
```

The `message_type` argument must follow the syntax: `daemon.type`.

`daemon`

It can take the following values: * (i.e. all daemons), `bdmaild`, `bdfiled`, `bdlogd`, `bdscand`, `bdmond`, `bdlived`

`type`

It can take the following values: * (i.e. all types), `info`, `error`, `license`, `debug`, `virus`, `spam`

You can also enable or disable the entire filelog plugin or just a certain type of message. To do this, run these commands as root:

```
# bdsafe logger file disable message_type  
# bdsafe logger file enable message_type
```

By default, the file log plugin appends the current UNIX time to the rotated file: `update.log.1237491868`, `update.log.1238491800` etc. A log file can be rotated as follows:

- By interval (hourly, daily, montly and multiple of them, like every 6 weeks).
- By size (ex: rotate when the size reaches 10 MB).

There's a another option called `Count` which determines how many log files are created.



Note

For a full description of the filelog settings you must take a look to the `bdsafe(8)` manual pages.

The SMTP log plugin

One of the main characteristics of the **bdlogd** plugins is the fact that they are easily and extremely configurable, by using the **bdsafe** command. Certainly, the SMTP log plugin makes no exceptions to the above-mentioned feature. You can find out the plugin status, enable / disable it, set a connection timeout, alert senders and receivers, choose a template or only a header, etc.

Let's take some examples.

If you want to find out the SMTP log plugin status (enable / disable, for the entire plugin or just for a certain type of messages) run the next command as root:

```
# bdsafe logger smtp status message_type
```

The `message_type` argument must follow the syntax: `daemon.type`.

`daemon`

It can take the following values: * (i.e. all daemons), `bdmaild`, `bdfiled`, `bdlogd`, `bdscand`, `bdmond`, `bdlived`, `bdsmtpd`

`type`

It can take the following values: * (i.e. all types), `info`, `error`, `license`, `debug`, `virus`, `spam`

To send a notification to the receivers of an infected email, run this command.

```
# bdsafe logger smtp alertrecv value
```



Note

For a full description of the SMTP log settings you must take a look to the `bdsafe(8)` manual pages.

The SNMP log plugin

By using the **bdsafe** command, you can get the SNMP log plugin status, enable /disable it, set the port number where notification will be sent, set a connection timeout, etc.

For example, to set the port number where notification will be sent, run this command as root:

```
# bdsafe logger snmp port value
```



Note

For a full description of the SNMP log settings you must take a look to the `bdsafe(8)` manual pages.

The SYSLOG logger plugin

Use the SYSLOG logger plugin to send all product specific messages to the system logger. Please see your distribution's documentation for information on how to filter these messages.

If you want to find out the SYSLOG plugin's status (enabled or disabled) for the entire range of messages or just for a certain type, then run the following command as root:

```
# bdsafe logger syslog status message_type
```

The `message_type` argument must follow the syntax: `daemon.type`.

`daemon`

It can take the following values: * (i.e. all daemons), `bdmaild`, `bdfiled`, `bdlogd`, `bdscand`, `bdmond`, `bdlived`, `bdsmtpd`

`type`

It can take the following values: * (i.e. all types), `info`, `error`, `license`, `debug`, `virus`, `spam`

You can also enable or disable the entire SYSLOG logger plugin or just a certain type of message. In order to do this, run these commands as root:

```
# bdsafe logger syslog enable message_type  
# bdsafe logger syslog disable message_type
```

To configure a user template for the specific message type, run this command as root:

```
# bdsafe logger syslog template message_type
```

11.6. Quarantine

The Quarantine is a special directory (or directories), unavailable for common users, where infected or suspected files or emails are to be isolated for a future purpose. Some Bitdefender Daemons (**bdmaild**, **bdfiled** and **bdbmond**) add files to Quarantine. The administrator can list and search these files, delete, restore or resend all files that match the given pattern by using the **bdsafe** command.

To find out information about Quarantine directories, run this command as root:

```
# bdsafe quarantine status [quarname]
```

If the optional `quarname` parameter is specified **bdsafe** will display information on that directory only.

To display all files from the `quarname` directory, run this command:

```
# bdsafe quarantine list [quarname]
```

Searching the Quarantine is also very easy. All you have to do is to run this line.

```
# bdsafe quarantine search [quarname] [field] [pattern]
```

The `field` parameter can take one of the following value:

- sender
- recipient
- subject
- uuid

 **Note** You can use wildcard (*) with the `pattern` parameter (except for the `uuid`).

To search the specified quarantine directory and copy, move or delete all files that match the specified pattern, run the appropriate command:

```
# bdsafe quarantine copy [quarname] [field] [pattern]
# bdsafe quarantine move [quarname] [field] [pattern]
# bdsafe quarantine delete [quarname] [field] [pattern]
```

The `field` parameter can take one of the following value:

- sender
- recipient
- subject
- uuid

Note

You can use wildcard (*) with the `pattern` parameter.

In case you want to resend all files that match the given pattern via the SMTP server, run this command:

```
# bdsafe quarantine resend [quarname] \  
[field] [pattern] server[:port] [crlfmagic]
```

The optional `crlfmagic` parameter can take any value. The effect of adding this parameter is the following one: **bdsafe** will actively replace all end-of-line sequences in the file with `\r\n`.

Important

If you resend the email through the same mail server that quarantined it, the email is going to be detected again and moved to quarantine. To successfully resend a quarantined email, you must use a different mail server. If you are using the SMTP proxy integration, it is possible to resend the email by using `localhost:10026` as the server parameter to the **bdsafe** command specified above. This will effectively skip the Bitdefender filter.

To handle the Quarantine configuration, run this command:

```
# bdsafe quarantine configure [quarname] [parameter] [value]
```

`parameter` can take one of the following value:

maxentries

It refers to the maximum number of files allowed in Quarantine.

In this case, the `value` parameter must be a positive integer.

maxsize

It refers to the maximum size of Quarantine allowed.

In this case, the `value` parameter must be a string describing the maximum size of the Quarantine directory. For example, `1m512k` specifies that the maximum size is 1.5 megabytes (`g` is for gigabytes, `m` for megabytes, `k` for kilobytes and `b` for bytes).

ttl

Time-to-live (`ttl`) refers to a certain time that, when exhausted, would cause the mail to be discarded from Quarantine.

In this case, the `value` parameter must be a string describing the maximum amount of time a file can remain in Quarantine before being deleted. For example, `1w2d` specifies that the maximum amount of time a file may remain in the quarantine is one week and two days (`w` is for weeks, `d` for days, `h` for hours, `m` for minutes, `s` for seconds).

12. THIRD PARTY INTEGRATION

With the release of the Bitdefender Security for Mail Servers SDK, advanced users have the possibility to write plugins and scripts that integrate with the product.

For more information, please refer to the `bdsms-sdk.tar.gz` file located in the `opt/Bitdefender/share` directory.

13. TESTING BITDEFENDER

To make sure Bitdefender Security for Mail Servers is really working, you can test its antivirus and antispam efficiency using standard testing methods. Basically, you will send a special email to some account through the email server. You will receive the results (disinfected email, notifications or the email marked as SPAM).

Sending the Email to Another Account

The `$USER` parameter is used to send the email to your current account on the local server. If you wish to send the test emails to another recipient or to some remote email server, replace it with a real email address, but take care the emails will be classified as infected and spam.

13.1. Antivirus Test

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

There is no reason to worry, because this file is not a real virus. All that `EICAR.COM` does when executed is 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 periodically test the server protection.

EICAR online resources

You can find out more and download the EICAR test file from the [EICAR website](#).

13.1.1. Infected Email Attachment

To test the email protection efficiency, create an email with your favorite email agent, attach the file `EICAR.COM` and send it to yourself through your email server. You will shortly receive the email disinfected, the notification emails that are supposed to reach you, the postmaster, and, if configured, the emails informing the sender and the receiver about the virus found.

Using the `mail` program, available on many Linux distributions, sending the email can be done in the following way. You can safely replace `mail` with `mutt`, or any other command that supports attachments.

```
$ echo "EICAR test file." | mail -s EICAR \  
-a EICAR.COM $USER
```

If your mail program does not support attachments, you can use the following command, where the email body is just the content of the `EICAR.COM` file (since it is an ASCII file). Having scanned the entire mail, Bitdefender Security for Mail Servers will find it infected, disinfect it and notify the postmaster and, eventually, the sender and the receiver.

```
$ mail -s EICAR $USER < EICAR.COM
```

13.1.2. Infected Attached Archive

To test the efficiency of the Bitdefender MIME Packer component, create an archive containing the `EICAR.COM` file, then attach it to an email sent to yourself through the email server to test. For example, `gzip` the `EICAR.COM` file and attach the resulting archive.

```
$ gzip --best EICAR.COM  
$ echo "EICAR test archive." | mail -s EICAR \  
-a EICAR.COM.gz $USER
```

You will shortly receive the disinfected email, the notification emails that are supposed to reach you, the postmaster, and, if configured, the emails informing the sender and the receiver about the virus found.

13.2. Antispam Test

You can verify that the Bitdefender Antispam component works properly by the help of a special test, known as *GTUBE*. GTUBE stands for the *Generic Test for Unsolicited Bulk Email*. GTUBE provides a test by which you can verify that the Bitdefender filter is installed correctly and it detects incoming spam.

GTUBE online resources

You can find out more and download the GTUBE test email (in RFC-822 format) from the [GTUBE website](#).

The test consists of entering the following 68-byte string, as one line, in the body of the email:

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

When scanning the email, Bitdefender Security for Mail Servers must tag it as spam.

Using any **mail** program, you can test Bitdefender Security for Mail Servers with the following command. You have to create a file, named `GTUBE`, containing the above string in one line. Then, run the following command.

```
$ nail -s GTUBE $USER < GTUBE
```

You will shortly receive the email marked as SPAM. The `Subject` and `X-BitDefender-Spam` headers will be:

```
Subject: [SPAM] GTUBE [SPAM]
X-BitDefender-Spam: Yes (100)
```

14. UPDATES

Bitdefender Security for Mail Servers was designed with capabilities for automatic update.

The Bitdefender update process is realized by Bitdefender Live! Update, a daemon which connects periodically to [the Bitdefender update server](#) and checks whether new virus definitions, antispam updates and product upgrades are available. In case there are any, the daemon will download only the changed files, executing an incremental update and saving bandwidth.

To find out the current configuration settings for the global proxy and the Bitdefender Live! Update service, run the following command.

```
# bdsafe live
```

14.1. Automatic Update

Bitdefender Security for Mail Servers is configured to update automatically each hour, through the **bdlived** module. In case of a necessary update, before the specified interval expires, the daemon can be signaled to execute the update routine, manually. To trigger the on-demand check, one can issue the following command.

```
# bdsafe live forceupdate
```

Note

A minimum of five minutes must elapse from the last forced update.

14.1.1. Time Interval Modification

To modify the time interval you will have to run the command bellow. You can change the update interval to the desired value, in seconds. The new value must be an integer between 3600 (seconds, 1 hour) and 86400 (seconds, 24 hours).

```
# bdsafe live checkinterval [new_value]
```

14.1.2. Bitdefender Live! Update Proxy Configuration

If a proxy server is to be used to connect to the Internet, you can set/get your proxy server address and port by using the following command.

```
# bdsafe live globalproxy host [new_host]
```

Without the optional [new_host] parameter, this command displays the current proxy host only, in case there is a proxy host. To change the host, you must add the [new_host] parameter, following this syntax: host[:port]

However, you have to enable proxy usage by this command.

```
# bdsafe live globalproxy enabled Y
```

In order to deactivate the use of a proxy, run the following:

```
# bdsafe live globalproxy enabled N
```

For proxy servers that require authentication, the server administrator can set the user domain, name and the associated password via the following commands:

```
# bdsafe live globalproxy user [new_user]
# bdsafe live globalproxy domain [new_domain]
# bdsafe live globalproxy password [new_password]
```

The Bitdefender Live! Update daemon does not immediately load the settings modified via the **bdsafe** command. So, a good idea would be to run the following command, to apply the configuration changes.

```
# bdsafe live reloadsettings
```

14.2. Manual Update

There is one zip archive on the update server, containing the updates of the scanning engines and virus signatures: [cumulative.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.

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

1. **Download the update file.** Please download `cumulative.zip` and save it somewhere on your disk when prompted.
2. **Extract the updates.** Extract the contents of the zip file to the `/opt/Bitdefender/var/lib/scan/Plugins/` directory, overwriting the existing files with the newer ones if necessary.
3. **Files owner and permissions.** After extracting the zip archive, you **must** set the proper owner and permissions, by running the following commands.

```
# chown bitdefender:bitdefender \  
/opt/Bitdefender/var/lib/Plugins/*  
  
# chmod 644 /opt/Bitdefender/var/lib/Plugins/*
```

4. **Restart Bitdefender.** Once updated, Bitdefender Security for Mail Servers should be restarted, using the following command.

```
# /opt/Bitdefender/bin/bd restart
```

14.3. PushUpdate

PushUpdate is an ordered update launched by Bitdefender servers in imminent situations, when a prompt update can save the server from allowing the infected emails to pass.

The trigger is an email, sent to the address you have to specify on <http://www.bitdefender.com/site/Products/pushUpdates/>. Bitdefender Security for Mail Servers, while filtering the emails, will recognize it and will initiate the update process.

14.4. Patches and New Product Versions

Since the Bitdefender Live! Update module can update automatically only the virus definitions and some of the core libraries used by Bitdefender, there is a small tool that can be used to update the whole Bitdefender installation.

BitDefender Swiss Army knife, **bdsafe(8)**, the multipurpose tool, can be used to keep Bitdefender up to date by applying various patches that might appear after the product was released. It can be run directly by the system administrator to list, search, install or uninstall patches or it can be installed as a cron job to automatically install patches as soon as they are released.

Patches are released to correct any bugs found or to add new features and they are grouped in the following categories: **CRITICAL**, **SECURITY**, **NORMAL**.

- Patches are labeled **CRITICAL** when they affect the normal behavior of the product. For example, if a new kernel is released, preventing the **bdcored** module to accomplish its job, then a **CRITICAL** patch will be released, correcting this issue.
- A patch is labeled **SECURITY** when it has the role of correcting any security related issue. For example, if there is a bug which might permit an attacker to gain access to emails scanned by Bitdefender, then a **SECURITY** patch will be released to fix this issue. As opposed to **CRITICAL** patches, which affect Bitdefender's normal behavior, **SECURITY** patches can fix the bugs that will not normally occur in a friendly environment, if such one exists.
- Patches labeled **NORMAL** are usually released to fix minor (cosmetic) bugs or to add some new features. For example, if Bitdefender incorrectly formats an email header, a **NORMAL** patch will be released to fix this minor issue.

New product versions may bring new features and functionalities. It is recommended to install upgraded versions when they become available.

Administrators are notified about releases of new patches and new product versions via automated emails, as well as through the Bitdefender Remote Admin interface. Notifications contain all the relevant information regarding the release, such as new features, bug fixes and installation instructions.



REMOTE MANAGEMENT

15. BITDEFENDER REMOTE ADMIN

Bitdefender Security for Mail Servers can be configured remotely by using a web browser. In order to do this, you need to install the Bitdefender Remote Admin module on the server side.

Bitdefender Remote Admin is an intuitive management interface. This management tool helps you remotely configure any settings in a single interface and lets you check the current status of the product (detailed statistics and update information).

When installing Bitdefender Remote Admin, you will be asked to enter a bind address for the Remote Admin server. For security reasons, by default, Bitdefender Remote Admin listens for incoming connections on `127.0.0.1` (port `8139`) and allows incoming connections from `127.0.0.1` only, as well. If you want to be able to remotely configure Bitdefender Security for Mail Servers, set the address to `0.0.0.0:8139` (listening on all interfaces).

To see the existing Remote Admin socket, run the following command:

```
# /opt/BitDefender/bin/bdsafe registry getkey \  
/BDUX/Radmin/Host
```

To set a new value for this socket, run the command:

```
# /opt/BitDefender/bin/bdsafe registry setkey \  
/BDUX/Radmin/Host [value]:8139
```

Before you use port number `8139`, make sure the port is not used by another application:

```
# netstat -anpe | grep 8139
```

Also as part of the installation you can set a password for the default administrator account. If you choose not to, the default password `admin` will be used.

Once the installation is completed, use the `bdcertgen.sh` script located in `/opt/BitDefender/bin/` to indicate your domain name and generate an openssl certificate file. It is highly recommended to enable SSL (Secure Sockets Layer)

connections when using remote administration, so make sure you have the `Net::SSLeay` perl module installed.

To start Bitdefender Remote Admin, run the following command:

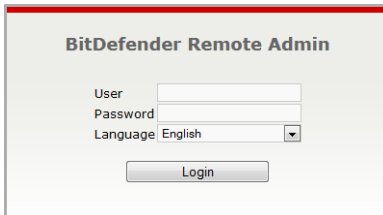
```
# /opt/BitDefender/bin/bdradmin start
```

After any modification to the configuration, you have to manually restart Bitdefender Remote Admin by running the following command:

```
# /opt/BitDefender/bin/bdradmin restart
```

15.1. Getting Started

Once you have setup Bitdefender Remote Admin, you can remotely configure almost all Bitdefender Security for Mail Servers settings. All you have to do is open your favorite web-browser and point it to the following location, for the standalone module: <https://your.domain.name:8139>. The following login form will appear:



BitDefender Remote Admin

User

Password

Language: English

Login

To login for the first time, use the default user account.



Note

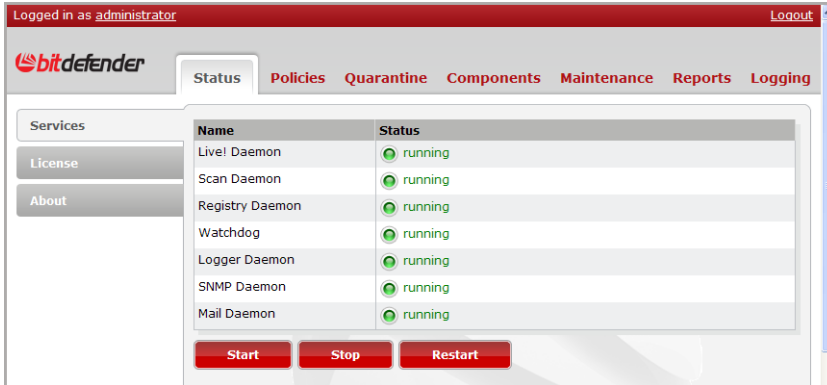
To change the default password, after logging in click **administrator** on the upper left-hand corner of the interface and type the new password in the provided textboxes.

The following sections of this document describe how to configure Bitdefender Security for Mail Servers using Bitdefender Remote Admin.

15.2. Status

15.2.1. Services

To open this section, go to **Status** and select **Services**.



The screenshot shows the Bitdefender Remote Admin interface. At the top, it says "Logged in as administrator" and "Logout". The main navigation bar includes "Status", "Policies", "Quarantine", "Components", "Maintenance", "Reports", and "Logging". The "Status" section is active, and the "Services" tab is selected. A table lists the following services and their status:

| Name | Status |
|-----------------|-----------|
| Live! Daemon | ● running |
| Scan Daemon | ● running |
| Registry Daemon | ● running |
| Watchdog | ● running |
| Logger Daemon | ● running |
| SNMP Daemon | ● running |
| Mail Daemon | ● running |

Below the table are three buttons: "Start", "Stop", and "Restart".

Services

Here you can see a list of all Bitdefender services and their current status. You can start, stop or restart the services by clicking the corresponding buttons.



Note

These actions are not performed instantly, a couple of seconds may be required for them to finish.

15.2.2. License

To open this section, go to **Status** and select **License**.

The screenshot shows the BitDefender Remote Admin interface. At the top, it says "Logged in as administrator" and "Logout". The main navigation bar includes "Status", "Policies", "Quarantine", "Components", "Maintenance", "Reports", and "Logging". The "Status" tab is selected. On the left, there are menu items for "Services", "License", and "About". The main content area is titled "BitDefender Security for Mail Servers". It displays the following information:

| | |
|-----------------------|---|
| Status | Evaluation version, 17 day(s) remaining |
| Licensed users | 10 |
| | Enter new license key |

Below this, there is a message: "Please contact your regional BitDefender reseller or go to our [website](#) to see a list of BitDefender partners in your area".

The "MyAccount" section is also visible, with the following options:

- Access an existing account**
 - E-mail address:
 - Password: [Forgot password?](#)
- Create a new BitDefender account**
 - E-mail address:
 - First name:
 - Password:
 - Last name:

License

Here you can check the license status and register Bitdefender Security for Mail Servers.

Click **Enter new license key**, type the license key in the corresponding textbox and click **Apply** to perform the registration process. If you mistype the license key, the message **Invalid key** will be displayed and you will have to type it again.

You can also create a Bitdefender account or login to an existing one to have access to technical support, keep your license keys safe, recover your lost license keys and take advantage of special offers and promotions.

To create a Bitdefender account, select **Create a new Bitdefender account** and provide the required information. The data you provide here will remain confidential.

- **Email address** - type your email address.
- **Password** - type a password for your Bitdefender account.



Note

The password must be at least four characters long.

- **Re-type password** - type again the previously specified password.
- **First name** - type your first name.
- **Last name** - type your last name.
- **Country** - select the country you reside in.

Click **Apply** to finish.



Note

Use the provided email address and password to log in to your account at <http://myaccount.bitdefender.com>.

To successfully create an account you must first activate your email address. Check your email address and follow the instructions in the email sent to you by the Bitdefender registration service.

15.2.3. About

To open this section, go to **Status** and select **About**.

The screenshot shows the BitDefender Remote Admin interface. At the top, it says "Logged in as administrator" and "Logout". The main navigation bar includes "Status", "Policies", "Quarantine", "Components", "Maintenance", "Reports", and "Logging". On the left, there is a sidebar with "Services", "License", and "About" (selected). The main content area is titled "BitDefender Common Components" and contains the following information:

| | | |
|--------------------|---|-----------------------|
| Description | Core components required by all BitDefender products. | |
| Version | 3.1.5 | |
| Components | Name | Version |
| | Registry Daemon | 3.10.0.140120 (27821) |
| | Watchdog | 3.10.0.131015 (27066) |
| | Logger Daemon | 3.10.0.140219 (28160) |
| | Live! Daemon | 3.10.0.140203 (28015) |
| | Scan Daemon | 3.10.0.140122 (27912) |
| | Management Client | 3.10.0.140127 (27986) |
| | Management | 3.10.0.140124 (27971) |
| | Swiss Army knife | 3.10.0.130411 (25294) |
| | SNMP Daemon | 3.10.0.140205 (28030) |
| | Core Library | 3.10.0.140220 (28197) |
| | Agents Configuration Plugin | 3.10.0.140307 (28308) |
| | Group Management Configuration Plugin | 3.10.0.140118 (27810) |
| | Information Plugin | 3.10.0.140116 (27756) |
| | License Management Plugin | 3.10.0.140116 (27756) |
| | Live! Daemon Configuration Plugin | 3.10.0.140123 (27944) |
| | Logger Daemon Configuration Plugin | 3.10.0.140220 (28188) |
| | Quarantine Management Plugin | 3.10.0.140305 (28290) |

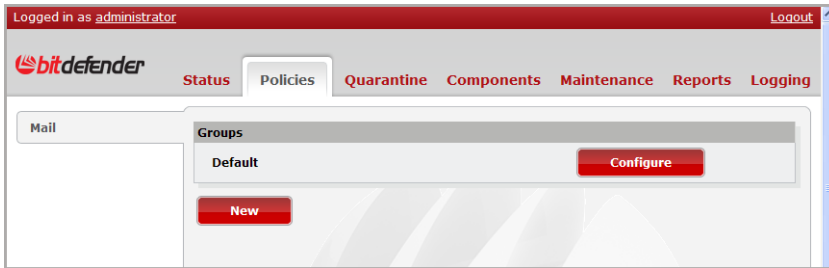
About

This section displays a short description, the version number and the list of components for every Bitdefender product installed.

15.3. Policies

When dealing with security policies you want to stay organized, work more efficiently and spend less time. To easily manage groups and enforce group security policies go to **Policies** and select **Mail**.

To manage the default security policy, go to **Policies** and select **Mail**.



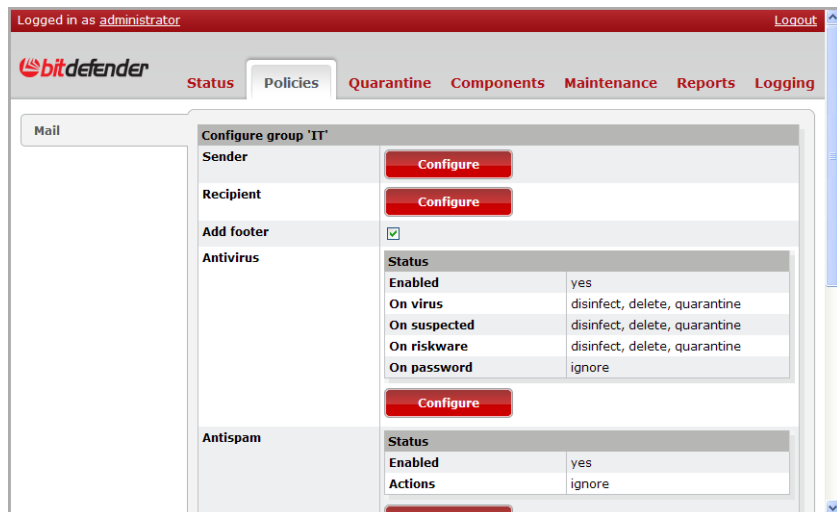
Policies

The list of groups is displayed in this window in order of their priority. To change the priority of a group, simply drag it up or down the list and drop it in the desired position.

To create a new group, click the **New** button, enter the group name and click **Add** to save the new group. To remove a group, click the **Delete** button corresponding to it.

15.3.1. Configuring Group Policies

You can edit the security policies for a group by clicking the **Configure** button corresponding to that group.



Configure Policies

The current settings are displayed for the selected group. You can manage the senders and recipients included in the group, configure the Antivirus, Antispam, Content Filter and Mail Forward.

Manage Groups

- **Sender** - to edit the list of email senders included in the group, click the corresponding **Configure** button.

Here you can see the list of senders currently assigned to the group. To add a new email address to the group, click the **New** button, enter the address and click **Add**. To remove a sender from the list, select the corresponding checkbox and click **Delete**. Click **OK** to save the changes to the group.

- **Recipient** - to edit the list of email recipients included in the group, click the corresponding **Configure** button.

Here you can see the list of recipients currently assigned to the group. To add a new email address to the group, click the **New** button, enter the address and click **Add**. To remove a recipient from the list, select the corresponding checkbox and click **Delete**. Click **OK** to save the changes to the group.



Note

When specifying email addresses, you can use the following wildcards to define an entire email domain or a pattern for email addresses:

- Asterisk (*), replacing zero, one or more characters.
- Question mark (?), replacing any single character.

Add Footer

Select the checkbox to enable the display of a message in the footer of emails which informs the recipients that the message was scanned by Bitdefender.

Antivirus

The settings of the Antivirus module are displayed in this section.

To edit the settings, click **Configure**.

The screenshot shows the Bitdefender Remote Admin interface. At the top, it says "Logged in as administrator" and "Logout". The main navigation bar includes "Status", "Policies", "Quarantine", "Components", "Maintenance", "Reports", and "Logging". The "Policies" tab is selected, and the "Mail" section is active. The configuration is for the "Configure the antivirus filter for group 'IT'".

| Category | Option | Status |
|--------------|--------------------|-------------------------------------|
| Enabled | Enabled | <input checked="" type="checkbox"/> |
| | Add headers | <input checked="" type="checkbox"/> |
| On virus | disinfect | <input checked="" type="checkbox"/> |
| | delete | <input checked="" type="checkbox"/> |
| | copy to quarantine | <input type="checkbox"/> |
| | move to quarantine | <input type="checkbox"/> |
| | drop | <input type="checkbox"/> |
| | reject | <input type="checkbox"/> |
| On suspected | disinfect | <input checked="" type="checkbox"/> |
| | delete | <input checked="" type="checkbox"/> |
| | copy to quarantine | <input type="checkbox"/> |
| | move to quarantine | <input type="checkbox"/> |
| | drop | <input type="checkbox"/> |
| On riskware | disinfect | <input checked="" type="checkbox"/> |
| | delete | <input checked="" type="checkbox"/> |
| | reject | <input type="checkbox"/> |
| | ignore | <input type="checkbox"/> |

Antivirus

- To enable the antivirus scanning of emails, select the corresponding checkbox.
- Bitdefender Security for Mail Servers can add a header to scanned emails. To enable headers, select the corresponding checkbox.
- Select the checkboxes next to the actions you want to be taken on **viruses**, **suspected objects** and **riskware**:

Disinfect

Remove the malware from the infected attachment (or any other mail component that can be used to send malware). If successful, the mail is passed to the next plugin (if any) or forwarded. Otherwise, the next action is executed.

Delete

Remove the attachment or other mail components that contain the malware. If successful, the mail is passed to the next plugin (if any) or forwarded. Otherwise, the next action is executed.

When the mail is completely deleted, a replacement letting the recipient know what happened will be generated.

Move to quarantine

Move the mail to quarantine. If the action fails, an error message line is written to the log.

After this action is taken, the mail will either be dropped or rejected.

Copy to quarantine

Copy the mail to quarantine. If the action fails, an error message line is written to the log.

Drop

Send the message to the mail transport agent (MTA) to drop the mail.

This action prohibits the mail from passing. The MTA will return no response to the sender.

Reject

Send the message to the mail transport agent (MTA) to reject the mail.

This action prohibits the mail from passing. However, the MTA will send back a rejection message.

Ignore

Send the message to the mail transport agent (MTA) to forward the mail.

- Select the checkboxes next to the actions you want to be taken on **password protected attachments**:

Copy to quarantine

Copy the mail to quarantine. If the action fails, an error message line is written to the log.

Move to quarantine

Move the mail to quarantine. If the action fails, an error message line is written to the log.

After this action is taken, the mail will either be dropped or rejected.

Drop

Send the message to the mail transport agent (MTA) to drop the mail.

This action prohibits the mail from passing. The MTA will return no response to the sender.

Reject

Send the message to the mail transport agent (MTA) to reject the mail.

This action prohibits the mail from passing. However, the MTA will send back a rejection message.

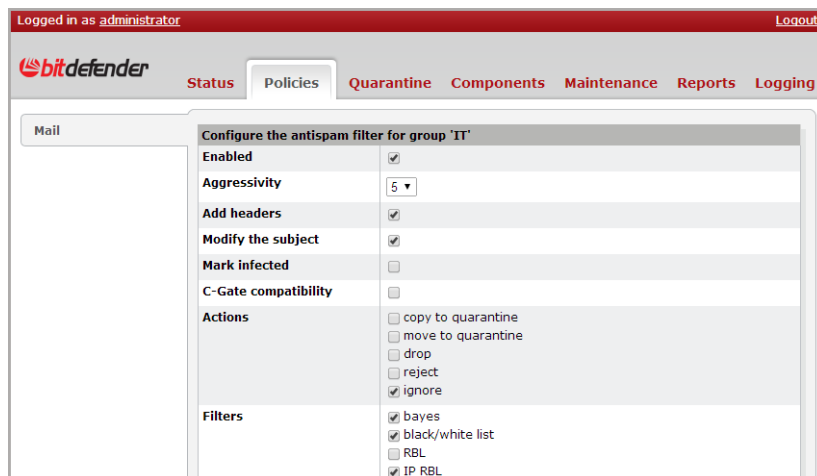
Ignore

Send the message to the mail transport agent (MTA) to forward the mail.

To save the changes, click **OK**.

Antispam

The Antispam settings are displayed in this section. To edit the settings, click **Configure**.



Antispam

- To enable the antispam filter, select the corresponding checkbox.
- To set the antispam **Aggressivity** level, use the corresponding drop-down list. The scale goes from 0 (minimum trust in antispam score returned by the Bitdefender filters) up to 9 (maximum trust). Choosing 0 might increase the amount of unsolicited emails, while choosing 9 might increase the amount of false positives. It is recommended to leave the default value (5) unchanged.
- **Add headers** will add new headers to all mails (by default X-BitDefender-Spam). The SpamStamp Header, by default X-BitDefender-SpamStamp, is a special feedback header, used by Bitdefender Antispam specialists as feedback, when false negatives and positives are submitted to spam_submission@bitdefender.com.
- Select **Modify subject** to modify the subject of the email messages conforming to the `Subject` template field.
- Select **Mark infected** to automatically mark as spam emails with infected attachments.
- Select **C-Gate compatibility** to add an X-Junk-Score header to emails, for compatibility with existent CommuniGate Pro filters. CommuniGate Pro uses

the value of the X-Junk-Score header to perform certain actions on the processed emails.



Note

For more information about the X-Junk-Score header, please refer to the CommuniGate Pro documentation.

- Select **Ignore the signature** to add the [SPAM] tag to email subject even if the detected spam email has a DomainKeys Identified Mail (DKIM) signature.
- Select the actions to be taken by the antispam filter:
 - Copy to Quarantine
 - Move to Quarantine
 - Drop
 - Reject
 - Ignore
- Each of the antispam filters can be enabled or disabled individually. Select the checkboxes corresponding to the filters you want to enable:
 - Bayes filter (no longer supported)
 - Black/White List filter
 - RBL filter
 - IP RBL filter
 - Multipurpose filter (Asian and Cyrillic charsets)
 - URL filter
 - Signatures filter
 - SURBL filter
 - Cloud filter
 - APM filter



Note

For more information, please refer to [Section 11.3 “Antispam Settings”](#) (p. 43).

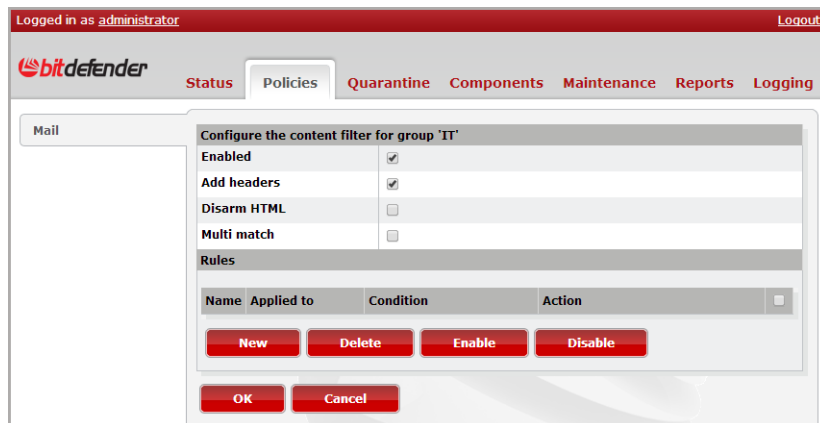
- Using the textboxes provided, you can add friends and spammers to the **White List** and **Black List** respectively. The entries may be usual email addresses or domain names (one entry per line), respecting the following format:

| Format | Description |
|-----------------|---|
| user@domain.com | This format will match only the specified user from the specified domain. |
| user@domain.* | The mentioned user from any domain whose name starts with the specified text will match. |
| user@*.com | The user from any domain with a .com suffix (for example) will match. |
| *@domain.com | This will match all users from the specified domain. |
| *@domain.* | All users from all domains starting with the mentioned text will match. |
| *.com | This will match all users from all domains with a .com suffix (for example). |
| user@* | The specified user, from all domains, will match. |
| user* | This will match all users whose names start with the mentioned text, no matter of the domain. |

To save the changes, click **OK**.

Content Filter

The Content filter settings are displayed in this section. To edit the settings, click **Configure**.



Content filter

- To enable the content filter or add a header to filtered emails, select the corresponding checkboxes.
- To remove potentially malicious code from emails containing HTML content, select the **Disarm HTML** checkbox.
- Enable **Multi match** if you want to check emails against all content filtering rules rather than stop further content filter processing once a rule is matched.
- The content filtering rules are listed in order of their priority under **Rules**. To change the priority of a rule, simply drag it up or down the list and drop it in the desired position.
- Select a rule and click **Delete** to remove it, **Enable/Disable** to enable/disable it, or **Edit** to configure the rule settings.
- To create a new content filtering rule, click the **New** button and follow these steps:
 1. Enter the rule name.
 2. Select the rule type. You can filter emails based on the following criteria: email headers, email body, email size, attachment MIME-type, attachment name (including extension), attachment size.

3. Select who will receive a notification from Bitdefender when a message matching the rule is detected: nobody (no notification is sent), the administrator, the recipient(s) or the sender.
4. Set the rule formula. The rule type will appear automatically in the **If** textbox. Select an expression from the adjoining drop-down list and enter a value for it in the textbox. To complete the formula, select an action from the **then** drop-down list: ignore, drop, reject, replace, copy to quarantine or move to quarantine.
5. Click **OK** to save the rule.

To save the changes, click **OK**.



Important

If you want to filter attachments based on their extension, use an attachment name rule and specify the necessary extensions using a regular expression, such as `[^\s]*\.(exe|scr|bat|com)`.

SMTP Forward

The mail forward settings are displayed in this section. To edit the settings, click **Configure**.

The screenshot shows the Bitdefender Remote Admin interface. At the top, it says "Logged in as administrator" and "Logout". Below the logo, there are navigation tabs: Status, Policies (selected), Quarantine, Components, Maintenance, Reports, and Logging. The main content area is titled "Mail" and contains a configuration window for "Configure the smtp forward for group 'IT'". The configuration includes:

| | |
|---------------|--|
| Enabled | <input type="checkbox"/> |
| Host | <input type="text" value="127.0.0.1"/> |
| Hello message | <input type="text"/> |
| From | <input type="text"/> |
| To | <input type="text"/> |
| When | <input type="text" value="before scan"/> |

At the bottom of the configuration window are two buttons: **OK** and **Cancel**.

SMTP forward

To enable message forwarding to another recipient, select the corresponding checkbox.

Next, specify the necessary information:

- IP / hostname
- Hello message
- From - the sender
- To - the destination account
- When - select from the drop-down list if you want the mails to be forwarded before or after being scanned

To save the changes, click **OK**.

After you are done configuring the policies for a group, click the **Apply** button to apply the changes.

15.4. Quarantine

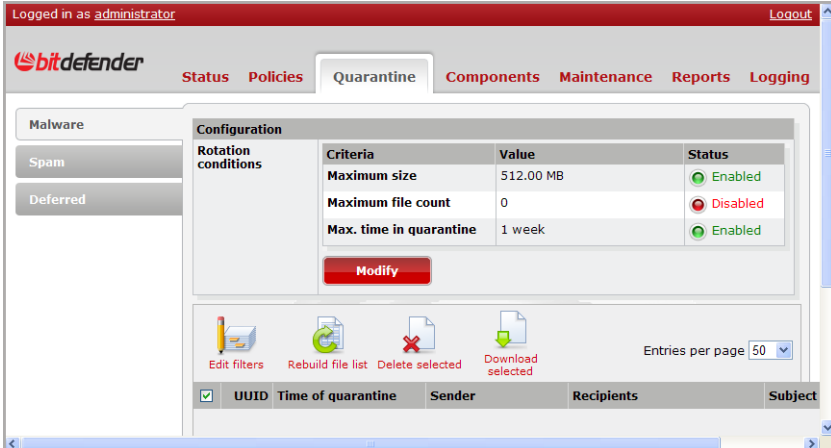
The Quarantine is a special directory, unavailable for common users, where suspected files or emails are to be isolated for a future purpose.

Quarantined objects are safe

When the virus is in Quarantine it can't do any harm, because it cannot be executed or read.

15.4.1. Malware Quarantine

To open this section, go to **Quarantine** and select **Malware**.



Logged in as administrator Logout

bitdefender Status Policies **Quarantine** Components Maintenance Reports Logging

Malware

Spam

Deferred

Configuration

| Rotation conditions | Criteria | Value | Status |
|---------------------|-------------------------|-----------|----------|
| | Maximum size | 512.00 MB | Enabled |
| | Maximum file count | 0 | Disabled |
| | Max. time in quarantine | 1 week | Enabled |

Modify

Edit filters Rebuild file list Delete selected Download selected

Entries per page 50

| <input checked="" type="checkbox"/> | UUID | Time of quarantine | Sender | Recipients | Subject |
|-------------------------------------|------|--------------------|--------|------------|---------|
|-------------------------------------|------|--------------------|--------|------------|---------|

Malware Quarantine

The Malware Quarantine is the directory where infected or suspected files are isolated from the system. The quarantine settings, status and contents are displayed in this window.

You can edit **Malware Quarantine Rotation Conditions** by clicking the **Modify** button and editing the textboxes corresponding to the following criteria:

- **Maximum size** - set a size limit for the quarantine directory. If you type just a number, the limit will be set in bytes. By adding **k**, **m** or **g** after the number you can set the size in Kilobytes, Megabytes or Gigabytes respectively.

- **Maximum file count** - set the maximum number of files the quarantine can contain at one time.
- **Maximum time in quarantine** - set the maximum period of time a file can spend in the quarantine. If you type just a number, the limit will be set in seconds. By adding *m*, *h*, *d* or *w* after the number you can set the time period in minutes, hours, days or weeks respectively.

To disable a condition, type 0 in its corresponding box. Click the **Apply** button to save the changes.

The contents of the quarantine are listed on the lower part of the window. For each item the UUID, time of quarantine, sender, recipients and subject are provided. You can use the following tools to easily browse and manage the quarantine:

- **Edit filters** - helps you filter the list of displayed items using the following criteria:
 - **Size** - display items of certain file sizes
 - **Time of quarantine** - display items added to the quarantine within a certain time interval
 - **Original file name** - display items with certain file names
 - **IP address** - display items originating from certain IP addresses
 - **Status** - display items infected by certain categories of malware
 - **Sender** - display items originating from certain email addresses
 - **Recipients** - display items delivered to certain email addresses
 - **Subject** - display items delivered in emails with certain subjects
 - **Infection** - filter items based on infection information:
 - **Virus** - display items affected by certain viruses
 - **Status** - display items with certain infection statuses
 - **Performed action** - display items that have been subjected to certain actions by the scanner
 - **Infected object** - display items that are found in certain locations.

Select the filtering options and click **Apply** to use them on the list.

- **Rebuild the list** - refresh the list of quarantined files.
- **Delete selected** - remove the selected items from the quarantine.

- **Download selected** - select quarantine items and download them to a location of your choice.
- You can choose how many items are to be displayed per page by selecting a number from the **Entries per page** drop-down list.

15.4.2. Spam Quarantine

To open this section, go to **Quarantine** and select **Spam**.

Logged in as administrator Logout

bitdefender Status Policies **Quarantine** Components Maintenance Reports Logging

Malware Spam Deferred

Configuration

| Criteria | Value | Status |
|-------------------------|-----------|----------|
| Maximum size | 512.00 MB | Enabled |
| Maximum file count | 0 | Disabled |
| Max. time in quarantine | 1 week | Enabled |

Modify

Edit filters Rebuild file list Delete selected Download selected Entries per page 50

| <input checked="" type="checkbox"/> | UUID | Time of quarantine | Sender | Recipients | Subject |
|-------------------------------------|------|--------------------|--------|------------|---------|
|-------------------------------------|------|--------------------|--------|------------|---------|

Spam Quarantine

This is where you will find the spam messages. The quarantine settings, status and contents are displayed in this window.

You can edit **Spam Quarantine Rotation Conditions** by clicking the **Modify** button and editing the textboxes corresponding to the following criteria:

- **Maximum size** - set a size limit for the quarantine directory. If you type just a number, the limit will be set in bytes. By adding **k**, **m** or **g** after the number you can set the size in Kilobytes, Megabytes or Gigabytes respectively.
- **Maximum file count** - set the maximum number of files the quarantine can contain at one time.
- **Maximum time in quarantine** - set the maximum period of time a file can spend in the quarantine. If you type just a number, the limit will be set in seconds. By

adding **m**, **h**, **d** or **w** after the number you can set the time period in minutes, hours, days or weeks respectively.

To disable a condition, type **0** in its corresponding box. Click the **Apply** button to save the changes.

The contents of the quarantine are listed on the lower part of the window. For each item the UUID, time of quarantine, sender, recipients and subject are provided. You can use the following tools to easily browse and manage the quarantine:

- **Edit filters** - helps you filter the list of displayed items using the following criteria:
 - **Size** - display items of certain file sizes
 - **Time of quarantine** - display items added to the quarantine within a certain time interval
 - **Original file name** - display items with certain file names
 - **IP address** - display items originating from certain IP addresses
 - **Sender** - display items originating from certain email addresses
 - **Recipients** - display items delivered to certain email addresses
 - **Subject** - display items delivered in emails with certain subjects
 - **SPAM Stamp** - display items with certain SpamStamp header values

Select the filtering options and click **Apply** to use them on the list.

- **Rebuild the list** - refresh the list of quarantined files.
- **Delete selected** - remove the selected items from the quarantine.
- **Download selected** - download the selected quarantine items to a location of your choice.
- You can choose how many items are to be displayed per page by selecting a number from the **Entries per page** drop-down list.

15.4.3. Deferred Quarantine

To open this section, go to **Quarantine** and select **Deferred**.

Logged in as administrator Logout

bitdefender Status Policies **Quarantine** Components Maintenance Reports Logging

Malware
Spam
Deferred

Configuration

| Rotation conditions | Criteria | Value | Status |
|---------------------|-------------------------|-----------|----------|
| | Maximum size | 512.00 MB | Enabled |
| | Maximum file count | 0 | Disabled |
| | Max. time in quarantine | 1 week | Enabled |

Modify

Edit filters Rebuild file list Delete selected Download selected

Entries per page 50

| <input checked="" type="checkbox"/> | UUID | Time of quarantine | Agent | For agent |
|-------------------------------------|------|--------------------|-------|-----------|
|-------------------------------------|------|--------------------|-------|-----------|

Deferred Quarantine

The Deferred Quarantine is an isolated directory storing all the objects that may cause process crashing (for instance, malformed archives or zip-bombs). The quarantine settings, status and contents are displayed in this window.

You can edit **Deferred Quarantine Rotation Conditions** by clicking the **Modify** button and editing the textboxes corresponding to the following criteria:

- **Maximum size** - set a size limit for the quarantine directory. If you type just a number, the limit will be set in bytes. By adding *k*, *m* or *g* after the number you can set the size in Kilobytes, Megabytes or Gigabytes respectively.
- **Maximum file count** - set the maximum number of files the quarantine can contain at one time.
- **Maximum time in quarantine** - set the maximum period of time a file can spend in the quarantine. If you type only a number, the limit will be set in seconds. By adding *m*, *h*, *d* or *w* after the number you can set the time period in minutes, hours, days or weeks respectively.

To disable a condition, type 0 in its corresponding textbox. Click the **Apply** button to save the changes.

The contents of the quarantine are listed on the lower part of the window. For each item the UUID, time of quarantine, agent and for agent are provided. You can use the following tools to easily browse and manage the quarantine:

- **Edit filters** - helps you filter the list of displayed items using the following criteria:
 - **Size** - display items that have certain file sizes
 - **Time of quarantine** - display items added to the quarantine within a certain time interval
 - **Original file name** - display items with certain file names
 - **Agent** - display items quarantined by certain Bitdefender Security for Mail Servers modules (i.e. **bdmond**)
 - **For agent** - display quarantine items detected by certain Bitdefender Security for Mail Servers modules

Select the filtering options and click **Apply** to use them on the list.

- **Rebuild the list** - refresh the list of quarantined files.
- **Delete selected** - remove the selected items from the quarantine.
- **Download selected** - download the selected quarantine items to a location of your choice.
- You can choose how many items are to be displayed per page by selecting a number from the **Entries per page** drop-down list.

15.5. Components

To open this section, go to **Components** and select **Mail**.

The screenshot shows the Bitdefender Remote Admin interface. At the top, it says "Logged in as administrator" and "Logout". The navigation menu includes "Status", "Policies", "Quarantine", "Components" (selected), "Maintenance", "Reports", and "Logging". The "Mail" section is active, showing a sidebar with "Mail" and a main configuration area. The configuration area is divided into sections: "General" with a "Realtime reporting" checkbox; "Antispam" with "Mark asian charsets" and "Mark cyrillic charsets" checkboxes; "RBL cache" with a "Flush" button; "RBL servers" with a table for "Server", "Trust", and "Delete" columns, and "New" and "Delete" buttons; "Spam submit" with "Enabled" checkbox, "Host" text field, "Use SSL" checkbox, "Interval" (5) seconds, "HAM user" and "SPAM user" fields with "password" labels, and "Apply" and "Revert" buttons at the bottom.

Components

To allow sending anonymous reports about the viruses and spam found on your server to the Bitdefender Lab, select the **Realtime reporting** checkbox. This way you can help Bitdefender identify new viruses and spam and find quick remedies for them.

15.5.1. Antispam

To mark messages written in Asian or Cyrillic characters as spam, select the corresponding checkboxes.

To clear the RBL cache, click the **Flush** button.

The RBL servers that are currently configured are listed under **RBL Servers**.

To add a new server, click **New** and enter the server name and the trust level (a value between 0 and 100) in the corresponding textboxes. Click **Add** to add the server to the list.

15.5.2. Spam Submissions

By allowing users to submit spam messages to the Bitdefender Lab you can help improve the pretrained Bayesian filter.

In order to use this feature, you have to configure its settings:

- Enable spam submissions by selecting the corresponding checkbox.
- Enter the POP3 host.
- Enable/disable SSL by selecting the corresponding checkbox.
- Set the time interval at which Bitdefender will check the account for emails.
- Enter the user name and, if required, the password for the SPAM and HAM user accounts.

15.5.3. SMTP

For SMTP Proxy integration, you have to specify the following information in order to allow Bitdefender to scan all email traffic:

- The real SMTP server address and port used by Bitdefender Security for Mail Servers to send the emails. By default the address is `127.0.0.1` and the port is `10025`.
- The port Bitdefender Security for Mail Servers will listen on. By default, the port is `25`.
- The connection timeout specifies how long Bitdefender will wait for incoming data through an already established connection before closing it.

Type the connection timeout value in seconds. For instance, if you type `60` and no data is transmitted across the already established connection for `60` seconds, Bitdefender will abort the connection. When the value is `0`, no timeout connection is enforced.

- The threads represent the maximum number of incoming concurrent connections Bitdefender will be able to handle. If the value entered is negative, all the incoming connection will be refused. When the value is `0`, no threads limit is enforced.
- The maximum size of the email messages that will pass through the SMTP Proxy. If a message size surpasses this limit, the email message will be rejected.

When the value is 0, no size limit is enforced. All the files, regardless of their size, will be scanned.

Networks

This section contains the networks Bitdefender relays email messages from. You must add the address in IPv4 format to the list, to instruct Bitdefender Security for Mail Servers to accept emails coming from these addresses, no matter of their destination.

The **New** button enables you to add one domain at a time. For each domain there is the option to delete it by selecting the checkbox and then clicking **Delete**.

Domains

The relay domains Bitdefender will use to accept emails for are configured in this section. For example, if your email server handles emails for the *company1.com* and *company2.com* domains, you must enter both domains in this section. If you have subdomains, you must specify them explicitly as *subdomain1.company3.com*, *subdomain2.company3.com*, etc.

The **New** button enables you to add one relay domain at a time. For each domain there is the option to delete it by selecting the checkbox and then clicking **Delete**.

Listen on

You can set a limit to the interfaces Bitdefender listen on, specified by their IP address. To add an address, click **New**, fill in the textbox and click **Add**. To remove an address, select the corresponding checkbox and click the **Delete** button.

15.6. Maintenance

15.6.1. Bitdefender Live! Update

To open this section, go to **Maintenance** and select **Bitdefender Live! Update**.

Logged in as administrator Logout

bitdefender Status Policies Quarantine Components **Maintenance** Reports Logging

Live! Update

Patches

Users

Global Proxy

General

Update server:

Update interval: seconds

Status

Last check: Wed 28 Oct 2009 12:46:57 PM UTC

Last update: Wed 28 Oct 2009 12:52:22 PM UTC

Antimalware

Core version: AVCORE v2.1 Linux/i386 11.0.0.29 (Aug 27 2009)

Signatures version: 7.28614

Signatures count: 4467939

Antispam

Bitdefender Live! Update

The Bitdefender Live! Update window provides information regarding the general update settings and update status, the malware signatures version and number of signatures and the Bitdefender Remote Admin version.

The default update server is <http://upgrade.bitdefender.com> and the default update interval is 1 hour. To use a different server or set a different time interval between updates, enter the new information in the corresponding textbox and click **Apply**.

Click the **Update Now!** button to trigger an automatic check and, possibly, update (if there are any updates on the server).

15.6.2. Patches

To open this section, go to **Maintenance** and select **Patches**. Patches might appear after the product is released. This is where you are provided with a list of available patches and a short description for each of them.

Choose which patches to install by selecting the checkbox next to them and click the **Update** button to start installing the selected patches.



Important

It is highly recommended to install product patches as soon as they are available.

15.6.3. Users

To open this section, go to **Maintenance** and select **Users**.

The screenshot shows the Bitdefender Remote Admin interface. At the top, it says "Logged in as administrator" and "Logout". The navigation menu includes Status, Policies, Quarantine, Components, Maintenance (selected), Reports, and Logging. On the left, there are buttons for Live! Update, Patches, Users (selected), and Global Proxy. The main content area is titled "User list" and contains a "General options" section with an "Add user" button. Below this is a table with the following details for a user named "radmin_manager":

| | |
|-------------|-----------------------------|
| User name | radmin_manager |
| Full name | Fullname |
| Permissions | ▸ Show detailed permissions |
| Options | Modify Delete |

Users

This is where you can create and manage Bitdefender Remote Admin user accounts. Existing users appear in the user list. To view the permissions of a user, click **Show detailed permissions**. To edit the credentials or permissions for a user, click the **Modify** button next to that user. To remove a user, click the **Delete** button.

To create a new user, click **Add user**.

Add New User

Fill in the necessary account information: the user name, the user’s full name and account password and set the permissions by selecting their corresponding checkboxes. Click the **Add user** button to finish.

15.6.4. Global Proxy

To open this section, go to **Maintenance** and select **Global Proxy**.

Global Proxy

This is where you can enter the proxy server settings.

If a proxy server is used to connect to the Internet, select the **Enabled** checkbox.

Enter the server address and port in the **Host** textbox. If authentication is required, you also have to enter the user name, password and domain in the corresponding textboxes.

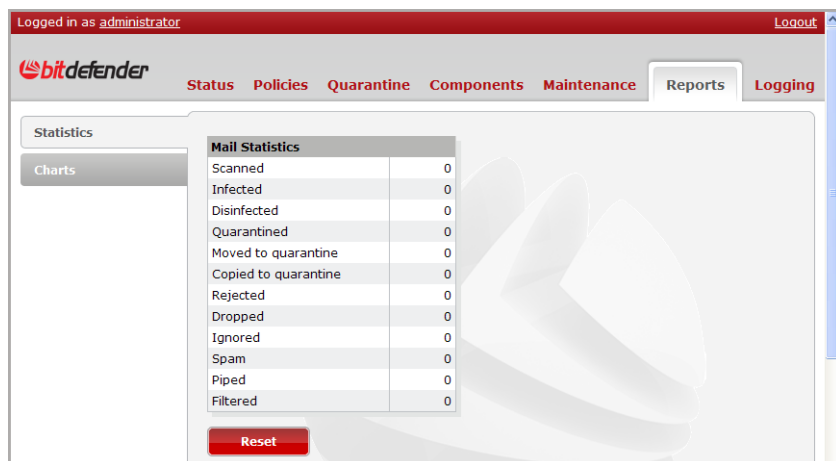
Click **Apply** to save the settings.

15.7. Reports

This section offers the possibility to obtain statistical data regarding product activity as well as showing helpful charts for information related to memory consumption and daemons activity.

15.7.1. Statistics

To open this section, go to **Reports** and select **Statistics**.



Logged in as administrator Logout

bitdefender Status Policies Quarantine Components Maintenance Reports Logging

Statistics

Charts

| Mail Statistics | |
|----------------------|---|
| Scanned | 0 |
| Infected | 0 |
| Disinfected | 0 |
| Quarantined | 0 |
| Moved to quarantine | 0 |
| Copied to quarantine | 0 |
| Rejected | 0 |
| Dropped | 0 |
| Ignored | 0 |
| Spam | 0 |
| Piped | 0 |
| Filtered | 0 |

Reset

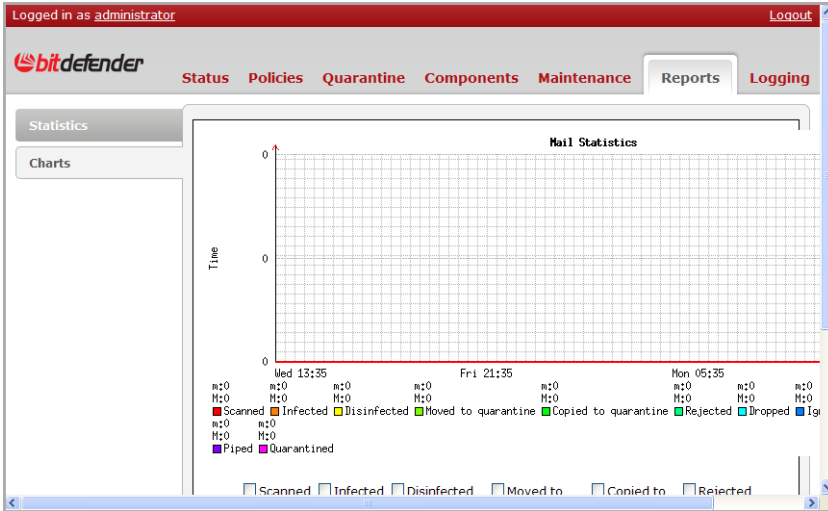
Statistics

The statistical report table can be accessed in this section. Here you can find information about scanned objects regarding their status and the action taken: Scanned, Infected, Disinfected, Quarantined, Rejected, Spam, Ignored, Dropped, Piped, Filtered.

Use the **Reset** button to clear the statistics.

15.7.2. Charts

To open this section, go to **Reports** and select **Charts**.



Charts

Here you can find two types of charts which you can select from the **Chart type** drop-down list:

- Resource Usage - provides information related to memory consumption and daemons activity
- Mail Statistics - provides information regarding actions taken on scanned objects

You can set which daemons' activity and which actions are to be displayed by selecting the corresponding checkboxes.

The charts can be customized by selecting different sizes from the **Chart size** drop-down list and different time intervals from the **Interval** drop-down list.

15.8. Logging

This section allows the customization of the logging process, realized by the Bitdefender logging module.

15.8.1. File Logging

To open this section, go to **Logging** and select **File Logging**.

The screenshot shows the Bitdefender Remote Admin interface. At the top, it says "Logged in as administrator" and "Logout". The navigation menu includes "Status", "Policies", "Quarantine", "Components", "Maintenance", "Reports", and "Logging". The "Logging" section is active, showing "File Logging" and "Mail Alerts" in the sidebar. The main content area has a "Add new rule" section with a form for "Component" (set to "[Any]"), "Rule type" (set to "[All]"), and "File name" (set to "/opt/BitDefender/var/log"). Below this is a table of "Existing rules".

| Component | Rule type | File name | Status |
|--------------|----------------------|------------------------------|---------|
| Live! Daemon | Information messages | /opt/BitDefender/var/log/up | Enabled |
| Live! Daemon | Error messages | /opt/BitDefender/var/log/up | Enabled |
| [Any] | Error messages | /opt/BitDefender/var/log/er | Enabled |
| [Any] | License information | /opt/BitDefender/var/log/lic | Enabled |
| | [All] | /opt/BitDefender/var/log/bc | Enabled |
| Mail Daemon | Spam | /opt/BitDefender/var/log/sp | Enabled |
| Mail Daemon | Detected viruses | /opt/BitDefender/var/log/vir | Enabled |
| Mail Daemon | Information messages | /opt/BitDefender/var/log/m | Enabled |

File Logging

By default, you will be provided with a list of logging rules. For each rule you can see the component (daemon) it applies to, the rule type, the location of the log file and the status. Enable/disable a rule by selecting the status from the corresponding drop-down list.

Let's say you enable the **Error messages** for **[Any]** component rule. This means that all error-related information, coming from all Bitdefender daemons, will be found in this location: `/opt/Bitdefender/var/log/error.log`. Of course, you can easily modify the location by editing the **File name** textbox.

If you want to add a new rule, select the component it applies to and the rule type from the corresponding drop-down lists, type the location of the file into the **File name** textbox and click **Add this rule**.

To complete the setup, click the **Apply** button. To use the default rule set, click the **Revert** button.

15.8.2. Mail Alerts

To open this section, go to **Logging** and select **Mail Alerts**.

The screenshot shows the Bitdefender Remote Admin interface. At the top, it says "Logged in as administrator" and "Logout". The navigation menu includes "Status", "Policies", "Quarantine", "Components", "Maintenance", "Reports", and "Logging". The sidebar has "File Logging" and "Mail Alerts" (selected). The main content area has a "Add new rule" section with dropdowns for "Component" (set to "[Any]") and "Rule type" (set to "[All]"), and a text input for "Email addresses". Below this is an "Add this rule" button. The "Existing rules" section contains a table with columns for Component, Rule type, Email addresses, and Status.

| Component | Rule type | Email addresses | Status |
|--------------|-----------------------------------|----------------------|----------|
| [Any] | Error messages | postmaster@ubuntu | Enabled |
| [Any] | License information | postmaster@ubuntu | Enabled |
| [Any] | New product version notifications | postmaster@ubuntu | Disabled |
| [Any] | New patch notifications | postmaster@ubuntu | Disabled |
| Mail Daemon | Detected viruses | | Disabled |
| Live! Daemon | New product version notifications | postmaster@localhost | Enabled |
| Live! Daemon | New patch notifications | postmaster@localhost | Enabled |

At the bottom of the main content area are "Apply" and "Revert" buttons.

Mail Alerts

Mail alerts are simple email messages sent by Bitdefender to the system administrator to inform him or her about special events or to the partners of an email communication to inform them about malware found.

By default, you will be provided with a list of logging rules. For each rule you can see the component (daemon) it applies to, the rule type, the email address and the status. Enable/disable a rule by selecting the status from the corresponding drop-down list.

If you want to add a new rule, select the component it applies to and the rule type from the corresponding drop-down lists, type the email address(es) the alerts should be sent into the **Email addresses** textbox and click **Add this rule**.

To complete the setup, click the **Apply** button. To use the default rule set, click the **Revert** button.

16. SNMP

16.1. Introduction

The SNMP (Simple Network Management Protocol) support of Bitdefender Security for Mail Servers consists of two implementations: a SNMP daemon and a Logger plugin.

The SNMP daemon is a custom implementation of a **snmpd** service. It exports a minimal set of features to allow interrogation of Bitdefender Security for Mail Servers.

The second implementation, the Logger plugin, is just another module besides the file logger, real-time virus and spam report module or mail notification module. It receives the same Bitdefender events information as the others Logger Plugins and it sends them to some remote host running the SNMP trap server, which, in its turn, will process them (send to syslog, etc.).

16.2. The SNMP Daemon

As stated before, this is a daemon that allows the user to interrogate the Bitdefender Security for Mail Servers settings.

One popular tool to do SNMP queries is **snmpget**, part of the **net-snmp** package. Each command must follow this syntax:

```
# snmpget -v 1 -Cf -c [community] [hostname] [OID]
```

Let's take an example. Suppose that you want to find out the number of scanned objects on `JohnDoe` server. Simply run this command.

```
# snmpget -v 1 -Cf -c initial JohnDoe \  
1.3.6.1.4.1.22446.1.1.1.1.1
```

Below you will find the complete list of the OIDs.

| Type | OID |
|-------------------------------|-------------------------------|
| Scanned | 1.3.6.1.4.1.22446.1.1.1.1.1.1 |
| Infected | 1.3.6.1.4.1.22446.1.1.1.1.1.2 |
| Disinfected | 1.3.6.1.4.1.22446.1.1.1.1.1.3 |
| Quarantined | 1.3.6.1.4.1.22446.1.1.1.1.1.4 |
| Dropped | 1.3.6.1.4.1.22446.1.1.1.1.1.5 |
| LastUpdate | 1.3.6.1.4.1.22446.1.1.1.2.1 |
| LastCheck | 1.3.6.1.4.1.22446.1.1.1.2.2 |
| CheckSecs | 1.3.6.1.4.1.22446.1.1.1.2.3 |
| License/Type | 1.3.6.1.4.1.22446.1.1.1.3.1.1 |
| License/Count (user) | 1.3.6.1.4.1.22446.1.1.1.3.1.2 |
| License/Count (domain) | 1.3.6.1.4.1.22446.1.1.1.3.1.3 |
| bdregd | 1.3.6.1.4.1.22446.1.1.3.1.1 |
| bdmond | 1.3.6.1.4.1.22446.1.1.3.1.2 |
| bdscand | 1.3.6.1.4.1.22446.1.1.3.1.3 |
| bdmaild | 1.3.6.1.4.1.22446.1.1.3.1.4 |
| bdlogd | 1.3.6.1.4.1.22446.1.1.3.1.5 |
| bdlived | 1.3.6.1.4.1.22446.1.1.3.1.6 |
| bdsmtpd | 1.3.6.1.4.1.22446.1.1.3.1.7 |
| bdmilterd | 1.3.6.1.4.1.22446.1.1.3.1.8 |

16.3. The Bitdefender Logger Plugin

The Bitdefender Logger receives messages from various Bitdefender Security for Mail Servers components and presents them to the user in various formats. It can log the messages to a file, forward them by email to a designated address or, using this plugin, it can send them to a SNMP server.

16.3.1. Prerequisites

You will need a working SNMP server installed on the same or on some other machine. Please take a look at the Troubleshooting section below, because there are some glitches you have be aware of.

You will also need the following MIB files present in the `mibs` directory we have talked about before:

- `BITDEFENDER-ALERTS-MIB.txt`
- `BITDEFENDER-NOTIFY-MIB.txt`
- `BITDEFENDER-TRAP-MIB.txt`

Regarding the SNMP protocol version, you can use 1, 2c or 3 with the following notes.

- Alerts of the `TRAP` type can be sent using the SNMP protocol versions 1 2c and 3.
- Alerts of the `INFORM` type can be sent using the SNMP protocol versions 2c and 3.
- Protocol 3 needs the user and offers authentication and encryption.
- Protocols 1 and 2c need no user, they use the `community` string, which is `public` by default.

16.3.2. Configuration

The messages sent to the SNMP server are received by the `snmptrapd` daemon. We need to configure it. But first, please make sure the SNMP services are not running.

We need a username for the SNMP version 3 protocol. If you want to use version 1 or 2c, you do not need the user and you can skip the following paragraphs.

Let's use the same `bitdefender` username as above. Make sure there is this line in the `/etc/snmp/snmpd.conf` file.

```
rwuser bitdefender
```

Thus we specify that this user who is not yet defined will have read and write access. Add this line at the end of the `/var/net-snmp/snmptrapd.conf` file

and remember the passwords should be longer than 8 characters. If the file does not exist, just create it.

```
createUser -e 0xBD224466 bitdefender MD5 <authpass> DES <privpass>
```

If you plan to use the `INFORM` alerts, without need for the `EngineID`, you will have to add a user without specifying the `EngineID`. The user defined in the line above will not work, so add a new one.

```
createUser bitdefender_inform MD5 <authpass> DES <privpass>
```

Let's stop a while and explain this line. You are free to change anything in it with the only condition to reflect the changes in the Bitdefender Security for Mail Servers configuration.

`-e 0xBD224466`

This is the `EngineID`. It is mandatory for alerts of the `TRAP` type and optional for the `INFORM` type. The alert type should be specified in the registry key `/BDUX/LoggerDaemon/Plugins/SNMP/AlertType`.

The `EngineID` must also be specified in the Bitdefender registry key `/BDUX/LoggerDaemon/Plugins/SNMP/SecurityEngineID`. If not used (it is optional when the alerts type is `INFORM`), the `SecurityEngineID` key must be empty.

`bitdefender`

This is the user to create for authenticated SNMP v3. The same name should be declared in the `/etc/snmp/snmpd.conf` (please read above) and in the registry key `/BDUX/LoggerDaemon/Plugins/SNMP/SecurityName`.

`MD5`

The authentication protocol (`MD5` or `SHA1`) used for authenticated SNMP v3. The same value must be found in the registry key `/BDUX/LoggerDaemon/Plugins/SNMP/AuthProto`.

`<authpass>`

Set the authentication pass phrase used for authenticated SNMP v3 messages. The same value must be found in the registry key `/BDUX/LoggerDaemon/Plugins/SNMP/AuthProtoPass`.

DES

Set the privacy protocol (DES or AES) used for encrypted SNMP v3 messages. The same value must be found in the registry key `/BDUX/LoggerDaemon/Plugins/SNMP/SecurityPrivProto`.

<privpass>

Set the privacy pass phrase used for encrypted SNMP v3 messages. The same value must be found in the registry key `/BDUX/LoggerDaemon/Plugins/SNMP/SecurityPrivProtoPass`.

This line will be replaced with another one, with encrypted passwords, when the **snmptrapd** daemon is started.

One more thing: you do not need to use all the parameters specified above for SNMP v3. You can use the authentication without encryption (the `SecurityLevel` key is `authNoPriv`) or no authentication and no encryption (the `SecurityLevel` key is `noAuthNoPriv`). You have to modify the `createUser` line accordingly.

This would be the user. Now, let's get back to the `/etc/snmp/snmpd.conf` file and add some more lines. You might find them already in your file, but commented out. Uncomment them and set the correct values.

```
# trapsink: A SNMPv1 trap receiver
trapsink localhost

# trap2sink: A SNMPv2c trap receiver
trap2sink localhost

# informsink: A SNMPv2c inform (acknowledged trap) receiver
informsink localhost public

# trapcommunity: Default trap sink community to use
trapcommunity public

# authtrapsenable: Should we send traps when authentication
# failures occur
authtrapsenable 1
```

I think this is the moment to start the **snmpd** and **snmptrapd** daemons. If you get an error, please review the configuration.

16.3.3. Usage

Now you can test the SNMP server. Here are some commands you may start with. The first one will send the `TRAP` alert that should be logged on syslog. Please note we use the EngineID.

```
# snmptrap -e 0xBD224466 -v 3 -m ALL -u bitdefender \  
-l authPriv -a MD5 -A <authpass> -x DES -X <privpass> \  
localhost 42 coldStart.0
```

Another command sends an `INFORM` alert. In this case, there is no need to specify the EngineID and the user you have created must not have the EngineID. In our examples, we have created the `bitdefender_inform` user for this purpose. The alert will be logged on the syslog too.

```
# snmpinform -v 3 -m ALL -u bitdefender_inform -l authPriv \  
-a MD5 -A <authpass> -x DES -X <privpass> localhost 42 \  
coldStart.0
```

If you do not want to use the SNMP version 3 protocol, you can use the other two supported: 1 and 2c. In this case you do not need the username, all you have to know is the community string. This is `public` by default. For example, for version 2c, use this command.

```
# snmptrap -c public -v 2c -m ALL localhost 42 coldStart.0
```

If everything is alright and Bitdefender Security for Mail Servers is properly configured (that means the registry keys fit the SNMP server configuration), all you have to do is to enable the plugin (if not already enabled) and try it by sending emails through the MTA. You will shortly see the report on the syslog of the machine running the SNMP server.

16.4. Troubleshooting

Due to some newly found bug in the `net-snmp` package, the `TRAP` feature does not work for `net-snmp` version 5.2.2 or newer with the SNMP version 3 protocol (but it works in version 5.2.1). This bug will hopefully be fixed by the `net-snmp` team soon.



GETTING HELP

17. SUPPORT

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



Note

You can find out information about the support services we provide and our support policy at the Support Center.

17.1. Bitdefender Support Center

[Bitdefender Support Center](#) is the place where you will find all the assistance you need with your Bitdefender product.

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

- Knowledge Base Articles
- Bitdefender Support Forum
- Product Documentation

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

Knowledge Base Articles

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

The Bitdefender Knowledge Base is open to the public and freely searchable. The extensive information it contains is yet another means of providing Bitdefender customers with the technical knowledge and insight they need. All valid requests for information or bug reports coming from Bitdefender clients eventually find their

way into the Bitdefender Knowledge Base, as bugfix reports, workaround cheatsheets or informational articles to supplement product helpfiles.

The Bitdefender Knowledge Base for business products is available any time at <http://www.bitdefender.com/support/business.html>.

Bitdefender Support Forum

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

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

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

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

Product Documentation

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

You can check and download the latest version of documentation for Bitdefender business products at [Support Center > Bitdefender Security for Mail Servers \(Linux\) > Documentation](#).

17.2. Asking for Assistance

You can contact us for assistance through our online Support Center:

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

18. CONTACT INFORMATION

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

18.1. Web Addresses

Sales Department: sales@bitdefender.com

Support Center: <http://www.bitdefender.com/businesshelp>

Documentation: documentation@bitdefender.com

Local Distributors: <http://www.bitdefender.com/partners>

Partner Program: partners@bitdefender.com

Media Relations: pr@bitdefender.com

Job Opportunities: jobs@bitdefender.com

Virus Submissions: virus_submission@bitdefender.com

Spam Submissions: spam_submission@bitdefender.com

Report Abuse: abuse@bitdefender.com

Web site: <http://www.bitdefender.com>

18.2. Local Distributors

The Bitdefender local distributors are ready to respond to any inquiries regarding their areas of operation, both in commercial and in general matters.

To find a Bitdefender distributor in your country:

1. Go to <http://www.bitdefender.com/partners>.
2. Go to **Partner Locator**.
3. The contact information of the Bitdefender local distributors should be displayed automatically. If this does not happen, select the country you reside in to view the information.
4. If you do not find a Bitdefender distributor in your country, feel free to contact us by email at sales@bitdefender.com. Please write your email in English in order for us to be able to assist you promptly.

18.3. Bitdefender Offices

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

United States

Bitdefender, LLC

PO Box 667588

Pompano Beach, FL 33066

United States

Phone (sales&technical support): 1-954-776-6262

Sales: sales@bitdefender.comWeb: <http://www.bitdefender.com>Support Center: <http://www.bitdefender.com/businesshelp>

Germany

Bitdefender GmbH

Airport Office Center

Robert-Bosch-Straße 2

59439 Holzwickede

Deutschland

Phone (office&sales): +49 (0)2301 91 84 222

Phone (technical support): +49 (0)2301 91 84 444

Sales: vertrieb@bitdefender.deWebsite: <http://www.bitdefender.de>Support Center: <http://www.bitdefender.de/businesshelp>

UK and Ireland

Genesis Centre Innovation Way

Stoke-on-Trent, Staffordshire

ST6 4BF

UK

Phone (sales&technical support): +44 (0) 8451-305096

Email: info@bitdefender.co.ukSales: sales@bitdefender.co.ukWebsite: <http://www.bitdefender.co.uk>

Support Center: <http://www.bitdefender.co.uk/businesshelp>

Spain

Bitdefender España, S.L.U.

Avda. Diagonal, 357, 1º 1ª

08037 Barcelona

España

Fax: (+34) 93 217 91 28

Phone (office&sales): (+34) 93 218 96 15

Phone (technical support): (+34) 93 502 69 10

Sales: comercial@bitdefender.es

Website: <http://www.bitdefender.es>

Support Center: <http://www.bitdefender.es/businesshelp>

Romania

BITDEFENDER SRL

DV24 Offices, Building A

24 Delea Veche Street

024102 Bucharest, Sector 2

Fax: +40 21 2641799

Phone (sales&technical support): +40 21 2063470

Sales: sales@bitdefender.ro

Website: <http://www.bitdefender.ro>

Support Center: <http://www.bitdefender.ro/businesshelp>

United Arab Emirates

Bitdefender FZ-LLC

Dubai Internet City, Building 17

Office # 160

Dubai, UAE

Phone (sales&technical support): 00971-4-4588935 / 00971-4-4589186

Fax: 00971-4-44565047

Sales: sales@bitdefender.com

Web: <http://www.bitdefender.com/world>

Support Center: <http://www.bitdefender.com/businesshelp>



APPENDICES

A. Supported Antivirus Archives and Packs

Bitdefender Security for Mail Servers scans inside the most common types of archives and packed files, including, but not limited to the following.

Supported archive types

| | |
|---------------------|---------------------|
| Ace | Jar |
| Arc | MS Compress |
| Arj | Lha (lzx) |
| bzip2 | Rar (including 3.0) |
| Cab | Rpm (clean+delete) |
| Cpio (clean+delete) | Tar (clean+delete) |
| Gzip (clean+delete) | Z |
| Ha | Zip (clean+delete) |
| Imp | Zoo |

Installation packers

| | |
|-----------------------|-----------------------------|
| Inno (Inno Installer) | InstallShield (ishield.xmd) |
| Instyler | Nullsoft Installer (NSIS) |
| VISE (viza.xmd) | Wise Installer |

Mail archives

Dbx (Outlook Express 5, 6 mailboxes)
Mbx (Outlook Express 4 mailbox)
Pst (Outlook mailboxes, supports clean and delete)
Mime (base64, quoted printable, plain) supports clean and delete
Mbox (plain mailbox - Linux and Netscape)
Hqx (HQX is a format used for mail attachments on Mac)
Uudecode
Tnef (a Microsoft format in which some properties of the attachments are encoded, and which can contain scripts)

Supported packers

| | |
|---|----------------------------|
| ACProtect / UltraProtect | PELock NT |
| ASPack (all versions) | Pencrypt (3.1, 4.0a, 4.0b) |
| Bat2exec (1.0, 1.2, 1.3, 1.4, 1.5, 2.0) | PePack (all versions) |

| | |
|---|--|
| Yoda's Cryptor | Perplex |
| CExe | PeShield |
| Diet | PeSpin |
| DxPack | Petite (all versions) |
| Dza | Pex |
| Patcher | PhrozenCrew PE Shrinker (0.71) |
| ECLIPSE | PkLite |
| Exe32Pack (1.38) | PKLITE32 (1.11) |
| ExePack | Polyene |
| ExeStealth | RelPack |
| JdProtect | Rjcrush (1.00, 1.10) |
| Lzexe | Shrinker (3.3, 3.4) |
| Mew | VgCrypt |
| Molebox (2.2.3, 2.2.4, 2.2.5, 2.2.6, 2.2.8) | Stpe |
| Morphine | Telock (all versions) |
| Neolite | T-pack |
| PC/PE Shrinker 0.71 | Ucexe |
| PCPEC | UPolyx |
| PE Crypt 32 (1.02 (a,b,c) | UPX (all versions) |
| PE PACK\CRYPT | WWPACK32 (1.0b9, 1.03, 1.12, 1.20) |
| PeBundle | Wwpack (3.01, 3.03, 3.04, 3.04PU, 3.05, 3.05PU) |
| pecompact (up to 1.40 beta 3) | Xcomor (0.99a, 0.99d, 0.99f (486), 0.99h, 0,99i) |
| PeDiminisher | |

Others

Chm (contains html which can be infected)

Iso (CD images)

Pdf

Rtf

Mso (contains compressed OLE2 files, this way macros are saved in case a Doc is saved as html)

Swf (extracts certain fields that contain various commands; these are scanned by other plugins, for ex: SDX)

Bach (extracts debug.exe scripts on the basis of heuristic methods)

Omf (object file)

B. Alert Templates

All alerts can be customized. Bitdefender Security for Mail Servers provides a template mechanism to generate the alert messages. These templates are plain text files containing the desired notice and certain variables, keywords, which will be replaced with their proper values during the alert generation.

B.1. Variables

The variables and their meaning are described in the table below.

| Variable | Description |
|-----------------------------------|---|
| <code>\${BitDefender}</code> | This variable will be replaced with the <i>BitDefender</i> string. |
| <code>\${RealSender}</code> | The sender of the email, taken from <code>MAIL FROM: SMTP</code> command. |
| <code>\${RealRecipients}</code> | The recipients of the email, taken from <code>RCPT TO: SMTP</code> command. |
| <code>\${HeaderSender}</code> | The sender of the email, from the <code>From:</code> header of the email. |
| <code>\${HeaderRecipients}</code> | The receivers of the email, from the <code>To:</code> and <code>Cc:</code> email headers. |
| <code>\${Subject}</code> | The subject of the alert email. |
| <code>\${Malware}</code> | The virus name. |
| <code>\${Object}</code> | The object containing the malware. |
| <code>\${Status}</code> | The status of the object, namely <i>Infected</i> , <i>Suspected</i> , <i>Unknown</i> . |
| <code>\${TakenAction}</code> | The action taken on the object. |
| <code>\${Days}</code> | The remaining period until key expiration. |
| <code>\${SenderIP}</code> | The IP address of the email sender (if available). |
| <code>\${MessageId}</code> | The contents of the "Message-Id" header (if found). |
| <code>\${Headers}</code> | The list of the "Received" headers (if found). |
| <code>\${TriedAction}</code> | The list of actions that the product was configured to take. |

| Variable | Description |
|---------------------------------------|--|
| <code>\${SpamScore}</code> | The email's spam score. |
| <code>\${SpamStamp}</code> | The antispam engines' stamp. The format and contents of this spam is not standardized and can change without notice. |
| <code>\${URL}</code> | The product's website. |
| <code>\${cfrule}</code> | The name of the matched content filtering rule. |
| <code>\${Newver.Product}</code> | The product name. |
| <code>\${Newver.Version}</code> | The product version. |
| <code>\${Newver.URL}</code> | The product download page. |
| <code>\${Newpatch.Priority}</code> | The patch priority (all, normal, security and critical). |
| <code>\${Newpatch.ID}</code> | The patch ID. |
| <code>\${Newpatch.Description}</code> | A short description of the path. |



The variable `${BitDefender}`

It is mandatory to include the variable `${BitDefender}` in your custom template. If it is not found, the module will use the built-in template instead.

These variables can be combined in any form inside the object lists in order to generate a custom template. By default, the templates are stored inside the `/opt/Bitdefender/share/templates` directory.

Regarding the email alerts, the involved templates are the following: `MailServerAlert.tpl`, `KeyHasExpiredAlert.tpl`, `KeyWillExpireAlert.tpl`, `ReceiverAlert.tpl` and `SenderAlert.tpl`.



The template name

You do not have to keep the default file name or location. The only mandatory thing is to refer it accordingly inside the Bitdefender Registry, under its corresponding key.

B.2. Sample Results

Looking inside the above-mentioned files, one could get confused about their structure. Here are the defaults for the English language and possible results when generating alerts.

B.2.1. MailServer Alert

This is the alert the postmaster will receive when an infected message is found. The variables that could be used are as follows.

- `${BitDefender}`
- `${RealSender}`
- `${RealReceivers}`
- `${HeaderSender}`
- `${HeaderRecipients}`
- `${Subject}`
- `${Virus}`
- `${Object}`
- `${Status}`
- `${Action}`

The default template is the following.

```
Subject: Virus warning!

${BitDefender} found an infected object in a message

Real sender: ${Mail.RealSender}

Real receivers: ${Mail.RealReceivers}

From: ${Mail.HeaderSender}

To: ${begin:Mail.HeaderRecipients}${Recipient} ${end}
```

```
Subject: ${Mail.Subject}
Virus: ${Malware}
http://www.bitdefender.com/site/Search?query=${Malware}
Object: ${Object}
Status: ${Status}
Action: ${TakenAction} (${TriedAction})

For more information please visit http://www.bitdefender.com/
```

This will expand into the following message (provided as an example).

```
Subject: Virus warning!

BitDefender found an infected object in a message

Real sender: <sender@example.com>
Real receivers: <receiver@example.com>
From: The Sender <sender@example.com>
To: The Receiver <receiver@example.com>
Subject: klez
Virus: Win32.Klez.A@mm
http://www.bitdefender.com/site/Search?query=Win32.Klez.A@mm
```

```
Object: /tmp/bdnp.milter.qf2aqW=>[Subject: klez]
```

```
Status: Infected
```

```
Action: Deleted
```

```
For more information please visit http://www.bitdefender.com/
```

B.2.2. Sender Alert

This is the alert the sender of the original email will receive when an infected message he has sent is found. Variables that could be used:

- `${BitDefender}`
- `${RealReceivers}`
- `${HeaderRecipients}`
- `${Subject}`
- `${Virus}`
- `${Object}`
- `${Status}`
- `${Action}`

The default template is the following.

```
Subject: Virus Warning!
```

```
${BitDefender} found an infected object in a message that was  
sent from your address
```

```
Real receiver: ${Mail.RealRecipients}
```

```
To: ${begin:Mail.HeaderRecipients}${Recipient} ${end}
```

```
Subject: ${Mail.Subject}
Virus: ${Malware}
http://www.bitdefender.com/site/Search?query=${Malware}
Object: ${Object}
Status: ${Status}
Action: ${TakenAction} (${TriedAction})

For more information please visit http://www.bitdefender.com/
```

This will expand into the following message (provided as an example).

```
Subject: Virus Warning!

BitDefender found an infected object in a message that was
sent from your address

Real receivers: <receiver@example.com>
To: The Receiver <receiver@example.com>
Subject: klez
Virus: Win32.Klez.A@mm
http://www.bitdefender.com/site/Search?query=Win32.Klez.A@mm
Object: /tmp/bdnp.milter.qf2aqW=>[Subject: klez]
```

```
Status: Infected
```

```
Action: Deleted
```

```
For more information please visit http://www.bitdefender.com/
```

B.2.3. Receiver Alert

This is the alert the receiver of the original email will get when an infected message having reached him is found. Variables that could be used:

- `${RealSender}`
- `${HeaderSender}`
- `${Subject}`
- `${Object}`
- `${Action}`
- `${Virus}`
- `${Status}`
- `${BitDefender}`

The default template is the following.

```
Subject: Virus warning!
```

```
${BitDefender} found an infected object in a message  
addressed to you:
```

```
Real sender: ${Mail.RealSender}
```

```
From: ${Mail.HeaderSender}
```

```
Subject: ${Mail.Subject}
```

```
Virus: ${Malware}
http://www.bitdefender.com/site/Search?query=${Malware}
Object: ${Object}
Status: ${Status}
Action: ${TakenAction} (${TriedAction})

For more information please visit http://www.bitdefender.com/
```

This will expand into the following message (provided as an example).

```
Subject: Virus warning!

BitDefender found an infected object in a message
addressed to you:

Real sender: <sender@example.com>
From: The Sender <sender@example.com>
Subject: klez
Virus: Win32.Klez.A@mm
http://www.bitdefender.com/site/Search?query=Win32.Klez.A@mm
Object: /tmp/bdnp.milter.qf2aqW=>[Subject: klez]
Status: Infected
```

```
Action: Deleted
```

```
For more information about BitDefender  
please visit http://www.bitdefender.com/
```

B.2.4. KeyWillExpire Alert

This is the alert the system administrator will receive when the license key is about to expire. Variables that could be used:

- `${Days}`
- `${BitDefender}`

The default template is the following.

```
Subject: Registration Info
```

```
Your BitDefender license will expire in ${Days} days!
```

```
For more information please visit http://www.bitdefender.com
```

B.2.5. KeyHasExpired Alert

This is the alert the system administrator will receive when the license key has expired. The variables that could be used are the next ones.

- `${BitDefender}`

The default template is the following.



Subject: Registration Error

Your BitDefender license has expired!

For more information please visit <http://www.bitdefender.com>

C. Footer Templates

Bitdefender Security for Mail Servers supports full customization of the footers appended to the emails and indicating whether they are clean or infected as well as extra detailed information about the infection. These footers are user-configurable: based on templates, they include several keywords, named *variables*, which will be replaced by the Bitdefender Security for Mail Servers notifying module with their corresponding values.

C.1. Variables

The variables and their meaning are described in the table below.

| Variable | Description |
|--|--|
| <code>#{BitDefender}</code> | This variable will be replaced with the <i>BitDefender</i> string. |
| <code>#{begin}</code> , <code>#{end}</code> | These are the markers of the object list boundary. Multiple object lists are allowed, provided they are not imbricated. |
| <code>#{object}</code> | The file or object found infected or suspected of being infected. |
| <code>#{status}</code> | The status of the object, namely <i>Infected</i> , <i>Suspected</i> , <i>Unknown</i> . |
| <code>#{virus}</code> | The virus name. If you want to know more about the reported virus, use the Virus Encyclopedia . |
| <code>#{action}</code> | The action taken for the object, namely <i>Disinfected</i> , <i>Deleted</i> , <i>Quarantined</i> , <i>Dropped</i> , <i>Rejected</i> , <i>Ignored</i> . Normally <i>Dropped</i> and <i>Rejected</i> should never appear, since these emails are lost. |



The variable `#{BitDefender}`

It is mandatory to include variable `#{BitDefender}` in your custom template. If it is not found, the module will use the built-in template instead.

These variables can be combined in any form inside the object lists in order to generate a custom template, no matter the language. By default, the templates are stored inside the `/opt/Bitdefender/share/templates/language` directory. For every supported language, there are subdirectory entries, such as `en`, `ro`, `de`,

fr, hu, es. Inside the language subdirectories, there are the template files, suggestively named.

Regarding the email footers, the involved template is `bd.tpl`.



The template name

You do not have to keep the default file name or location. The only mandatory thing is to refer it accordingly inside the Bitdefender Registry, under its corresponding key.

C.2. Sample Results

Looking inside the above-mentioned file, one could get confused about the structure. Here are the defaults for the English language and possible results when generating the footers.



Text encoding

To avoid strange output results, the text must be written using the plain ASCII character set, since there is no charset encoding conversion.

The default template is as follows.

```
-----  
  
This mail was scanned by ${BitDefender}  
  
For more information please visit http://www.bitdefender.com  
  
${begin:virus}  
  
Found virus:  
  
    Object: ${object}  
  
    Name:   ${virus}  
  
    Status: ${status}  
  
    Action: ${action}
```

```
#{end}
```

C.2.1. Clean

When the message is clean, the footer will as follows.

```
This mail was scanned by BitDefender
```

```
For more informations please visit http://www.bitdefender.com
```

C.2.2. Ignored

When an infected email is found and the action was to ignore that object, the result is the following.

```
This mail was scanned by BitDefender
```

```
For more information please visit http://www.bitdefender.com
```

```
Found virus:
```

```
Object: (MIME part)=>(application)=>word/W97M.Smac.D
```

```
Name: W97M.Smac.D
```

```
Status: Infected
```

```
Action: Ignored
```

C.2.3. Disinfected

Finally, when an infected email was found and cleaned, the result will read as follows.

```
This mail was scanned by BitDefender
```

```
For more information please visit http://www.bitdefender.com
```

```
Found virus:
```

```
Object: (MIME part)=>(application)=>word/W97M.Story.A
```

```
Name: W97M.Story.A
```

```
Status: Infected
```

```
Action: Disinfected
```

Glossary

ActiveX

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

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

Archive

A disk, tape, or directory that contains files that have been backed up.

A file that contains one or more files in a compressed format.

Backdoor

A hole in the security of a system deliberately left in place by designers or maintainers. The motivation for such holes is not always sinister; some operating systems, for example, come out of the box with privileged accounts intended for use by field service technicians or the vendor's maintenance programmers.

Boot sector

A sector at the beginning of each disk that identifies the disk's architecture (sector size, cluster size, and so on). For startup disks, the boot sector also contains a program that loads the operating system.

Boot virus

A virus that infects the boot sector of a fixed or floppy disk. An attempt to boot from a diskette infected with a boot sector virus will cause the virus to become active in memory. Every time you boot your system from that point on, you will have the virus active in memory.

Browser

Short for Web browser, a software application used to locate and display Web pages. The two most popular browsers are Netscape Navigator and Microsoft Internet Explorer. Both of these are graphical browsers, which means that they

can display graphics as well as text. In addition, most modern browsers can present multimedia information, including sound and video, though they require plugins for some formats.

Command line

In a command line interface, the user types commands in the space provided directly on the screen, using command language

Cookie

Within the Internet industry, cookies are described as small files containing information about individual computers that can be analyzed and used by advertisers to track your online interests and tastes. In this realm, cookie technology is still being developed and the intention is to target ads directly to what you've said your interests are. It's a double-edge sword for many people because on one hand, it's efficient and pertinent as you only see ads about what you're interested in. On the other hand, it involves actually "tracking" and "following" where you go and what you click. Understandably so, there is a debate over privacy and many people feel offended by the notion that they are viewed as a "SKU number" (you know, the bar code on the back of packages that gets scanned at the grocery check-out line). While this viewpoint may be extreme, in some cases it is accurate.

Disk drive

It's a machine that reads data from and writes data onto a disk.

A hard disk drive reads and writes hard disks.

A floppy drive accesses floppy disks.

Disk drives can be either internal (housed within a computer) or external (housed in a separate box that connects to the computer).

Download

To copy data (usually an entire file) from a main source to a peripheral device. The term is often used to describe the process of copying a file from an online service to one's own computer. Downloading can also refer to copying a file from a network file server to a computer on the network.

Email

Electronic mail. A service that sends messages on computers via local or global networks.

Events

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

False positive

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

Filename extension

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

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

Heuristic

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

Internet Protocol (IP)

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

Memory

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

Non-heuristic

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

Packed programs

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

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

Path

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

The route between any two points, such as the 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.

System tray

Introduced with Windows 95, the system tray is located in the Windows taskbar (usually at the bottom next to the clock) and contains miniature icons for easy access to system functions such as fax, printer, modem, volume, and more. Double click or right click an icon to view and access the details and controls.

Transmission Control Protocol/Internet Protocol (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 into your computer.

The term comes from a story in Homer's Iliad, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

Update

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

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

Virus

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

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.