

# BitDefender Security for Mail Servers

EVALUATOR'S GUIDE



## 1. Quick Summary

<i>BitDefender Security for Mail Servers</i>	
TAG LINE	Comprehensive antimalware protection for UNIX-based Mail Servers
PLATFORMS	Linux, FreeBSD
DESCRIPTION	Designed for UNIX-based mail servers, 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 e-mail platforms, the solution offers your company reliable protection against newly emerging malware and attempts to steal confidential and valuable data.
AVAILABILITY	April, 2008 (English version)

## 2. Solution Description

Designed for UNIX-based mail servers, 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 e-mail platforms, the solution offers your company reliable protection against newly emerging malware and attempts to steal confidential and valuable data.

### Key Features

- Fast and easy deployment
- Easy integration with your current mail services
- Compatible with most major e-mail platforms
- Proactive heuristic protection against zero-day threats
- Multiple layers of antispam filtering
- Content and attachment filtering
- Antispymware and antiphishing protection
- Intuitive program interface

## 3. Main Benefits and Features

### *E-mail Protection against Malware*

- Fights e-mail-borne malware by filtering and blocking messages that carry dangerous active codes
- Offers anti-phishing protection by proactively detecting forged messages intended to trick their recipient into disclosing confidential data
- 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, qmail and CommuniGate Pro
- Fully complies with FHS (Filesystem Hierarchy Standard), operating in a completely non-intrusive manner
- Ensures compatibility with all major Unix-based platforms due to its rpm, deb and generic .tar.run packages

### *Increased Business Productivity*

- Reduces mail traffic and saves network resources due to its extensive antimalware protection capabilities
- Through its optimized scanning process, increases mail delivery speed and reduces server workload
- 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
  - blocks unsolicited mail based on several filters, among which:
    - the Bayesian Filter, which you can train to learn the specifics of spam e-mail received by your server
    - the Real-time Blackhole List (RBL) filter, which identifies spam based on mail servers' reputation as spam senders

- Allows configuring antispam filter sensitivity by setting very demanding or relaxed thresholds for each user group
- 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 e-mail 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 Plug-in
- Can send virus and administration alerts to three different hosts, through the SNMP Logger plug-in

## ***4. Services***

### ***Advanced Update System***

For permanent mail protection, BitDefender Security for Mail Servers receives the latest updates and patches based on four configurable technologies: on-demand, scheduled, automatic and pushed.

### ***Upgrades***

Registered users benefit from free upgrades to any new version of the solution during the license period. Special pricing is always provided to our customers when they renew their license, making BitDefender a long-term, cost effective solution.

### ***Free 24/7 Professional Technical Support***

Certified representatives provide BitDefender business customers with free permanent support on-line, by telephone or e-mail. This is supplemented by an on-line database with answers to Frequently Asked Questions and fixes for common issues.

## 5. System Requirements

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

### 5.1. Hardware system requirements

#### Processor type

x86 compatible, minimum 800MHz, but do not expect a great performance in this case. An i686 generation processor, running at 1.4Ghz, would make a better choice.

#### Memory

The minimum accepted value is 128MB (recommended is at least 256MB, for a better performance).

#### Free disk space

The minimum free disk space to install and run BitDefender Security for Mail Servers is 60MB. But the log and the quarantine directories will require more space - 200MB of free space would be welcome.

#### Internet connection

Although BitDefender Security for Mail Servers will run with no Internet connection, the update procedure will require an active HTTP link, even through some proxy server. Therefore, for an up to date protection, the Internet connection is a MUST.

### 5.2. Software system requirements

#### Linux requirements

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

BitDefender requires `glibc` version 2.3.1, or newer, and `libstdc++` from `gcc` 3.2.2 or newer.

The supported Linux distributions are the next ones.

- RedHat enterprise Linux 3 or newer
- SuSE Linux Enterprise Server 9 or newer
- Suse Linux 8.2 or newer
- RedHat Linux 9
- Fedora Core 1 or newer
- Debian GNU/Linux 3.1 or newer
- Slackware 9.x or newer
- Mandrake/Mandriva 9.1 or newer
- Gentoo 1.4 or newer

## **FreeBSD requirements**

The supported FreeBSD versions are 5.4-RELEASE or newer.

The FreeBSD older versions are no longer supported.

## **5.3. Mail servers minimum required versions**

### **Sendmail**

version 8.12.1, with Milter interface

### **Postfix**

any 2.x version

### **qmail**

1.03 version at least

### **Courier**

0.42.x versions at least

### **CommuniGate Pro**

4.1.1 version at least

### **SMTP**

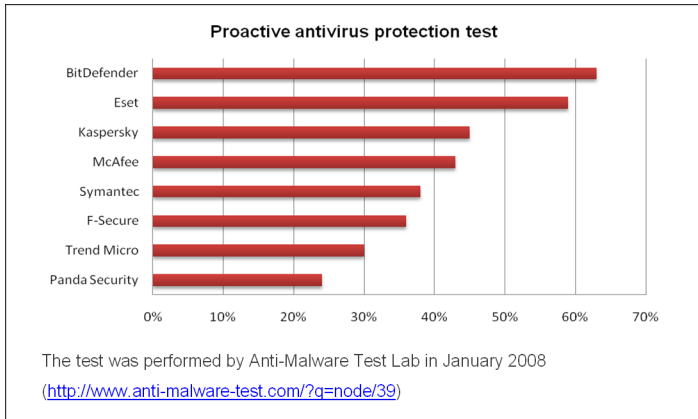
any SMTP server able to listen on another port than 25

## **6. Technology Leadership**

### **B-HAVE**

All BitDefender business solutions include B-HAVE, a patent pending technology which analyzes the behavior of potentially malicious codes inside a virtual computer, eliminating false positives and significantly increasing detection rates for new and unknown malware.

Proactivity is a measure of how well an antivirus copes with new and previously-unknown threats. The chart below represents the percentage of threats detected exclusively based on their behavior (rather than on the traditional, virus signature method).



## NEUNET

The new antispam filter available in BitDefender Total Security 2008 uses a Neural Network (a concept borrowed from the field of Artificial Intelligence) to deal with the new spam messages sent every day. Its main advantage is that it can recognize new spam by perceiving similarities (oftentimes very subtle) between the new messages received and the ones it was trained on.

## Image Spam Filter

BitDefender offers a more accurate image filter which, instead of analyzing the text within image spam messages, learns the common characteristics of those images in point of colour content and proportions. The result: less false positives and lower spam traffic.

## 7. Test Recommendations

### 7.1. Package installation

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

### Getting BitDefender Security for Mail Servers

The package can be downloaded from the BitDefender servers or it can be found on different distribution media, such as CD-ROM. When downloading from the BitDefender

servers, you will be asked to fill in a form and you will receive an email on the address you have provided in this form. The email contains the download location.

The Linux package come in three flavours.

- `rpm` for distributions using the RedHat Linux package management
- `deb` for distributions using Debian Linux packaging system
- `ipk` for any other distribution using IPKG, the Itsy Package Management System

The FreeBSD packages are `tbz` (`.tar.bz`) compressed archives, adequate for FreeBSD starting from version 5.

## Install the package

There is a common method of install, for `rpm`, `deb` and `ipk`, as well as several methods for FreeBSD.

### Install the Linux packages

The packages should be installed using the following command.

```
# sh BitDefender-Security-Mail-{ver}.{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 files (engines, core, etc.), the install and uninstall scripts.

Let's take some examples.

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

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

To install BitDefender Security for Mail Servers on a Debian based distribution you have to run the following command.

```
# sh BitDefender-Security-Mail-{ver}.{os}.{arch}.deb.run
```

The `ipk` version of the archive will install the `ipkg` tools on the system and will use them to install the `.ipk` packages.

To install BitDefender Security for Mail Servers on any Linux distribution, using `ipkg`, you have to run the following command.

```
# sh BitDefender-Security-Mail-{ver}.{os}.{arch}.ipk.run
```

## Additional parameters

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

<i>Parameter</i>	<i>Description</i>
<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.
<code>--uninstall</code>	Run the embedded uninstaller script instead of the normal installer.

## Install the FreeBSD package

To install BitDefender Security for Mail Servers on a FreeBSD machine, you have two methods: you can install the packages you have downloaded from the BitDefender servers or you can install them from the ports collection.

## Install the downloaded packages

To install the downloaded packages, run the following command in their directory.

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

## Install the language package

You have the possibility to choose the language you are familiar with at install time. By doing so, the help messages, error messages, etc. will be displayed in accordance with your choice.

To install the language package on your computer, you just have to run the following command.

```
# sh BitDefender-Security-Mail-langpack-{ver}.{os}.\  
  {arch}.{pkg}.run
```

It automatically detects the language of the system locale via the LANG environment variable.

The language localization files will be placed under the following directory: /opt/BitDefender/share/locale/[lang]/.

A link pointing to /opt/BitDefender/share will be made as /usr/share/bitdefender.

However, if you are dissatisfied with the chosen language, you can configure this option, setting another language to display in. This can be done either by changing the value of the LANG variable or by using a configuration key together with **bdsafe** tool.

This is the command you should run if you have decided to use **bdsafe** tool.

```
# bdsafe lang LL_CC.UTF-8
```

LL stands for language code (ISO 639) and CC for country code (ISO 3166). For example, if you want to set the language to display in to be Romanian, run the command:

```
# bdsafe lang ro_RO.UTF-8
```



## **Important**

Your terminal must support **UTF-8** encoding.

If you didn't install the language pack in the first place, just install it through the package manager any time you like.

## **The installer**

After unpacking the archive, the installer is launched. This is a text based installer, created to run on very different configurations. Its purpose is to install the extracted packages to their locations and to make the first configuration of BitDefender Security for Mail Servers, while asking you few questions. To accept the default configuration the installer offers (which is recommended), just press the `ENTER` key when prompted.

First, 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.

Next, on Linux, you are asked what integration agents to install. You can choose one or more from this list.

1. CommuniGate Pro
2. Courier
3. Sendmail Milter
4. qmail
5. SMTP Proxy (for Postfix or any other MTA)

Please enter the corresponding numbers, when prompted, separated by empty spaces. For example, to install the integration agents for *Sendmail Milter* and *qmail*, enter `3 4`.

The next question regards the RBL feature. You will be asked to specify the DNS server and one or more RBL servers.

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 Linux system.

- Creates the `bitdefender` user and group and assigns the installation directory to it.

- Installs the manpages and configures the `MANPATH` accordingly.
- Appends to the dynamic library loader configuration file the path to the BitDefender libraries.
- Creates a symbolic link to the configuration directory in `/etc`.
- Integrates BitDefender in the system init scripts.
- Finally, BitDefender Security for Mail Servers is started-up.

## 7.2. Configuration

### 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.

### 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.

There are two special groups: `All` and `Default`. The `All` group concentrates the settings for all users, as expected, and the `Default` group specifies the implied settings, if they are not defined in a certain group.

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

First, a new group has to be created. Let's name it `MyGroup` and add an 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 MyGroup sender:user1@example.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.

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 MyGroup
```

Let's add a recipient user.

```
# bdsafe group insert MyGroup 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 MyGroup antivirus actionsonvirus \  
'disinfect;quarantine'
```

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

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

Let's use the `Default` group, too: by default, the email footers should not be appended. Here is the command.

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

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 MyGroup
```

## Integration with LDAP server

The process of creating groups can be easily simplified when you integrate the BitDefender Security for Mail Servers with a 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 `Group_Name` 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.

## The Default Settings

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  = ''
smtprcpt  = ''
smtpip    = '127.0.0.1'
smtpport  = ''

Configuration for 'antivirus', group 'Default':
enable     = 'Y'
addheaders = 'Y'
headername = 'X-BitDefender-Scanner'
actionsonriskware = 'copy-to-quarantine;reject'
actionsonsuspected = 'copy-to-quarantine;reject'
actionsonvirus = 'copy-to-quarantine;reject'
pipeprogram = ''
pipeprogramarguments = ''

Configuration for 'antispam', group 'Default':
enable     = 'Y'
addheaders = 'Y'
modifysubject = 'Y'
aggressivity = '0'
actions     = 'move-to-quarantine'
whitelist  = '/opt/BitDefender/etc/as_wlist'
blacklist  = '/opt/BitDefender/etc/as_blist'
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'
usebfilter = 'Y'
usebayesfilter = 'Y'
useheurfilter = 'Y'
useimgfilter = 'Y'
usemultifilter = 'Y'
usepbayesfilter = 'Y'
userblfilter = 'Y'
useurlfilter = 'Y'
usesignfilter = 'Y'
pipeprogram = ''
pipeprogramarguments = ''
```

```

Configuration for 'contentfilter', group 'Default':
enable           = 'Y'
rules            = '/opt/BitDefender/etc/cf/Default-cf.conf'
maxrules         = '1000'
administrator    = ''
smtpserver       = ''
    
```

Each settings will be explained in the following table.

| <i>Setting</i>               | <i>Value</i>                                                                                  |
|------------------------------|-----------------------------------------------------------------------------------------------|
| AddFooters                   | Y if it is enabled, N if it is disabled. Add a new footer to all mails or not.                |
| SmtptForward/Enable          | Y if you forward mails to another mail server, N if SmtptForward is disabled.                 |
| SmtptForward/When            | Shows if the mail messages are to be forward to another mail server before or after scanning. |
| SmtptForward/SMTP_HELO       | Shows the other mail server HELO protocol command.                                            |
| SmtptForward/SMTP_FROM       | Shows the other mail server MAIL FROM protocol command.                                       |
| SmtptForward/SMTP_RCPT_TO    | Shows the other mail server RCPT TO protocol command.                                         |
| SmtptForward/SMTP_IP         | Shows the other mail server IP address.                                                       |
| SmtptForward/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.                                 |
| 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.                           |

| <b>Setting</b>                  | <b>Value</b>                                                                                                                                                                 |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.                                                                                                                              |
| 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 | Y if the antispam Bayesian filter is enabled, N if it is disabled.                                                                                                           |

| <b>Setting</b>                   | <b>Value</b>                                                                                                             |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Antispam/Engines/UseHeurFilter   | Y if the antispam heuristic filter is enabled, N if it is disabled.                                                      |
| Antispam/Engines/UseIMGFilter    | Y if the antispam image filter is enabled, N if it is disabled.                                                          |
| Antispam/Engines/UseMultiFilter  | Y if the antispam multi-filter is enabled, N if it is disabled.                                                          |
| Antispam/Engines/UsePBayesFilter | Y if the antispam pre-trained Bayesian 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/PipeProgram             | Shows the full path to the program to pipe the mail to.                                                                  |
| 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 `All` group and to any new created group.

## 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 `All` group, containing the entire list of users, both senders and receivers, and a special group, the `Default` one.

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 to ignore malware and illicit messages for the `Dangerous` group.

Each group was created with a specified priority. For example, the `Secretary` group was created with priority 4.



### Note

Remember that the `All` group has by default the 1 priority (the highest priority).

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

| Group     | Priority |
|-----------|----------|
| All       | 1        |
| 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 `All` 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 `All` 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.

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

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

```
# bdsafe group priority All 8
```

The group priority order will be now the following one.

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

Please notice that it make 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.

## 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 change 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 set 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.

## 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 `GROUP_NAME`. 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 `GROUP_NAME`. When applied, this rule means that emails containing in their body words like `salary`, `salaries`, `salarry`, `salariaess`, `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[iaou]nk</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.         |
| <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.                                  |

| Example                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <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-ID[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 `GROUP_NAME`. 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 modify 0 "priority=3" "name=porn rule"
```

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

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

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

```
6. | # bdsafe group configure GROUP_NAME \  
    | contentfilter dump
```

This will list the content filter rules of GROUP\_NAME together with their priorities.

```
7. | # bdsafe group configure GROUP_NAME \  
    | contentfilter delete 4
```

This will delete the content filter rule of GROUP\_NAME with priority 4.

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

This will disable the content filter rule of GROUP\_NAME with priority 4.

## 7.3. Testing BitDefender

To make sure BitDefender is really working, you can test its antivirus and antis spam 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 machine. 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.

## 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 visit the EICAR website at <http://eicar.com/>, read the documentation and download the file from one of the locations on the web page [http://eicar.com/anti\\_virus\\_test\\_file.htm](http://eicar.com/anti_virus_test_file.htm).

## **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 will find it infected, disinfect it and notify the postmaster and, eventually, the sender and the receiver.

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

## **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.

## 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 visit the *GTUBE* website at <http://gtube.net/>, read the documentation and download the sample RFC-822 format email from the locations on the web page.

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 must tag it as spam.

Using any **mail** program, you can test BitDefender 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)
```

## 7.4. Uninstall

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

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

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

## Uninstall the ipk package

To uninstall BitDefender Security for Mail Servers using ipkg, you have to run the following commands.

```
# ipkg-cl remove bitdefender-mail
# ipkg-cl remove bitdefender-common
```



### Note

The ipkg command must be run from the following location: /opt/ipkg/bin/

## Alternative uninstall

You can also uninstall the product this way:

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

## Uninstall the FreeBSD package

There are two ways to uninstall FreeBSD packages, depending on the installation method.

## Uninstall a locally downloaded package

To uninstall the packages you have installed from a local download, run the following commands.

```
# pkg_delete bitdefender-mail-{ver}  
# pkg_delete bitdefender-common-{ver}
```

Or, using `pkg_deinstall`, part of `sysutils/portupgrade`, run the following command.

```
# pkg_deinstall bitdefender-mail bitdefender-common
```

## 8. BitDefender Awards and Certifications

BitDefender solutions consistently earn top marks from independent testing organizations and are recognized by top industry publications.



## 9. Contact Info

Main site: <http://www.bitdefender.com/>  
Sales department: [sales@bitdefender.com](mailto:sales@bitdefender.com)  
On-line Store: <http://www.bitdefender.com/site/Buy/products/>  
Find a distributor: <http://www.bitdefender.com/site/Partnership/list/>  
Technical support: [support@bitdefender.com](mailto:support@bitdefender.com)

### **BITDEFENDER LLC**

6301 NW 5th Way Suite 3500 Fort Lauderdale, FL 33309  
Phone: 954.776.6262, 800.388.8062  
Fax: 954.776.6462, 800.388.8064