

# BitDefender Security for Samba

EVALUATOR'S GUIDE



## 1. Quick Summary

<i>BitDefender Security for Samba</i>	
TAG LINE	Efficient Antimalware Protection for Samba Network Shares
PLATFORMS	Linux, FreeBSD
DESCRIPTION	BitDefender Security for Samba provides antivirus and antispysware protection for Samba network shares. By scanning all accessed files for known and unknown malware it keeps network users safe and it helps comply with data protection regulations. Highly flexible, the open source BitDefender vfs module can be compiled against any Samba version, rendering it the ideal choice for your favorite Unix-based system.
AVAILABILITY	April, 2008 (English version)

## 2. Solution Description

### Key Features

- Proactive heuristic protection against zero-day threats
- Supports different actions or settings for each protected share
- SNMP monitoring systems support
- Flexible and intuitive remote management interface
- Complies with all major Linux distributions

## 3. Main Benefits and Features

### Compatibility

- Features a pre-compiled version of the vfs module, allowing integration with the latest Samba build available
- Works with any Samba build and can be easily compiled against all versions, thanks to its open-sourced vfs module

- 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

## ***Safe Sharing of Files and Documents***

- Enables safe file and document sharing by adapting its actions to the malware type detected
- Provides the possibility of separately handling riskware (applications that pose a potential threat, but which certain user groups might still need)
- Uses a built-in "Pipe to program" action, which allows you to feed the objects detected by the BitDefender engines to scripts or to other programs
- Allows you to define more than one quarantine area, searchable based on regular expressions, sender, recipient, date and cause for quarantine

## ***Increased Usability***

- Allows you to define separate sets of antivirus rules for each protected share resulting in better compliance with specific file sharing policies
- Allows performing management actions via SNMP by means of its SNMP Daemon Plug-in
- Can send customizable e-mail notifications or SNMP alerts about its activity: number of scanned, disinfected, deleted, infected or filtered files
- Comes with an intuitive management interface, BitDefender Remote Admin, which helps remotely configure any settings and check the current or past activity of the solution (detailed statistics, graphs and charts)
- Offers an alternative command line interface, BDSAFE (The BitDefender Swiss Army Knife), which allows performing post-install configuration and administration tasks

## ***Centralized Management Support***

BitDefender Management Server allows centralized management for most BitDefender business solutions installed on network computers, including BitDefender Security for Samba. This type of integration allows you to use the Management Server console to get centralized access to:

- configuration settings for BitDefender Security for Samba

- critical event information such as update-related events, configuration warnings, license expiration
- easy-to-interpret statistics and reports based on the information received from BitDefender Security for Samba

## 4. Services

### *Advanced Update System*

For permanent mail protection, BitDefender Security for Samba 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 Samba, 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 Samba 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 Samba 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. File server requirements

At the release date, BitDefender Security for Samba fully supports Samba version 3.x. Further versions will be supported as they appear. If you have another version and there is no precompiled BitDefender VFS module, you have to get the sources from `/opt/BitDefender/var/src` directory and compile them by yourself. For more about this, please see the install notes accompanying the BitDefender VFS module.

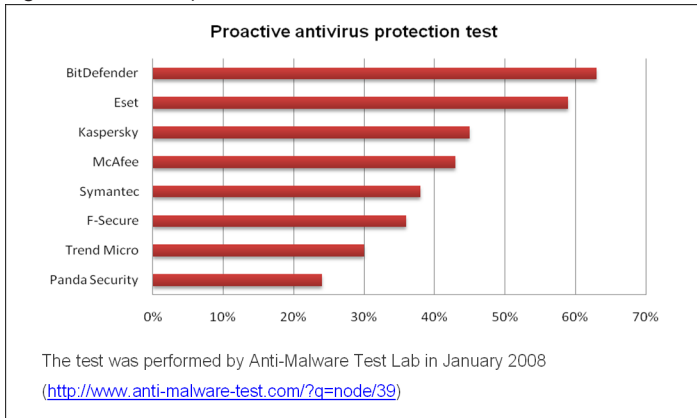
If you do not have Samba installed, you must download the source code, compile and install it.

## 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 Samba

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 Ipsy 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-Samba-{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 Samba on a RedHat based distribution you have to run the following command.

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

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

```
# sh BitDefender-Security-Samba-{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 Samba on any Linux distribution, using **ipkg**, you have to run the following command.

```
# sh BitDefender-Security-Samba-{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.

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>

<i>Parameter</i>	<i>Description</i>
<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 Samba 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-Samba-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 Samba, 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.

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 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 Samba is started-up.

## 7.2. Fileserver Integration

Due to the internal Samba architecture, the BitDefender VFS can work with only one version of Samba, the one which it was built for. Therefore, the full file name respects the following rule: `bdvfs-{samba_version}.so`, where `{samba_version}` represents the version of Samba the module was built for, such as `3.0.10`. If the package does not contain the VFS module you need for your Samba server, please use the sources from `/opt/BitDefender/var/src` to compile a compatible module.

After the installation you will get an up and running file server virus scanner. To complete the configuration and protect the shares, please refer to the “*Basic Configuration*” (p. 12) section.

If your Samba sources used for compiling VFS module differ from the Samba installed on your Linux distribution, the VFS module should be symlinked into Samba VFS directory. Regarding Samba installation, the location of VFS directory may vary. Depending on your setup, usual locations might be: `/usr/lib/samba/vfs` or `/usr/local/samba/lib/vfs`. The symlink MUST have the name `bdvfs3.so`. To create it, use the following command, replacing the paths and version according to your configuration.

```
# ln -sf /opt/BitDefender/var/lib/samba-vfs/bdvfs-3.0.x.so \\  
/usr/lib/samba/vfs/bdvfs3.so
```

Finally, start `smbd` daemon (for example run `smbd -D` as root).

## Compiling Samba

If you like to compile Samba, you may follow this example.

- Download the Samba source package, for example `samba-3.0.10.tar.gz`, then run this commands.

```
$ wget http://us4.samba.org/samba/ftp/old-versions/samba-3.0.10.tar.gz  
$ tar zxf samba-3.0.10.tar.gz && cd samba-3.0.10/source  
$ ./configure --prefix=/usr/local --with-smbmount --with-syslog  
$ make headers  
$ su -  
# make install
```

- Restore your Samba configuration back in `/etc/samba`. You may run **testparm** to check your `smb.conf` file. If **testparm** does not find `smb.conf` file, you must create a symlink in `/usr/local/lib` pointing to the actual `/etc/samba/smb.conf` file.

## Basic Configuration

Here are some hints on fine tuning BitDefender Security for Samba. We will use the **bdsafe** tool for this.

To check the configuration status, run this line.

```
# bdsafe samba status
```

You can see or set the actions to be taken by File Daemon on all malware categories (infected, suspected and riskware), by running this command.

```
# bdsafe samba actions [newactions]
```

The `newactions` parameter must be specified as a list of comma-separated action names. Valid action names are: `disinfect`, `copy-to-quarantine`, `move-to-quarantine`, `delete`, `deny` and `ignore`.

However, you can set the actions to be taken by File Daemon on a particular type of malware, by running one of the following commands.

```
# bdsafe samba oninfected [newactions]
```

```
# bdsafe samba onsuspected [newactions]
```

```
# bdsafe samba onriskware [newactions]
```

Also, you can set the actions to be taken by File Daemon when the first action failed. Run this command.

```
# bdsafe samba failureaction [ignore|deny]
```

## Samba VFS Module Configuration

By default, the `smb.conf` file is in a pre-defined location (`/etc/samba/smb.conf` for Linux and `/usr/local/etc/smb.conf` for FreeBSD). You can override this default hard-coded search path by running the following command.

```
# bdsafe samba vfs confpath [newpath]
```

The `newpath` parameter must be the fully-qualified path to the `smb.conf` file, not the directory in which the `smb.conf` file is located (e.g. `/etc/smb.conf` not `/etc`).



### Note

The BitDefender Registry Service must be running in order to change the `smb.conf` file location.

To find out detailed information on the status of the BitDefender Samba VFS module, run this command.

```
# bdsafe samba vfs status [sharename]
```

If the optional `sharename` parameter is specified, the information is displayed for that share only.

The BitDefender Samba VFS module is activated/deactivated on a per-share basis. You can activate/deactivate it by running one of the following commands.

```
# bdsafe samba vfs enable [sharename]
```

```
# bdsafe samba vfs disable [sharename]
```

At the same time, you can define a different set of actions to be taken for each share, based on malware type, by running one of the following commands.

```
# bdsafe samba vfs oninfected [sharename] [newacts]
```

```
# bdsafe samba vfs onsuspected [sharename] [newacts]
```

```
# bdsafe samba vfs onriskware [sharename] [newacts]
```

You can set the failure action for the Samba share specified by the `sharename` parameter, by running the following command.

```
# bdsafe samba vfs failureaction [sharename] [newval]
```

## 7.3. Testing BitDefender

To make sure BitDefender is really working, you can test its antivirus efficiency using standard testing methods. Basically, you will try to access a special file on a protected fileserver. According to your configuration, you will be allowed or denied access and the file will be disinfected, quarantined, removed or kept in place.

### 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\ZX54(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).

## 7.4. Uninstall

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

First, do not forget to remove the lines you have added to the Samba shares in the `/etc/samba/smb.conf` configuration file. You should remove `bdvfs3` from the `vfs` `objects` line or even the entire line if no other objects are used. Remove also the configuration lines of `bdvfs3` from the same file, if any. They start with something like `bdvfs3:`.

## Uninstall the rpm package

To uninstall BitDefender Security for Samba on an `rpm` package manager based distribution, you have to run the following commands.

```
# rpm -e BitDefender-samba
# rpm -e BitDefender-common
```

## Uninstall the deb package

To uninstall BitDefender Security for Samba using `dpkg`, on a `deb` package manager based distribution, you have to run the following commands.

```
# dpkg -r BitDefender-samba
# dpkg -r BitDefender-common
```

## Uninstall the ipk package

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

```
# ipkg-cl remove BitDefender-samba
# ipkg-cl -r 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-Samba-{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-samba-{ver}
# pkg_delete bitdefender-common-{ver}
```

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

```
# pkg_deinstall bitdefender-samba 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