

BitDefender for MS Exchange 2003

User Guide



Table of Contents

License and warranty	5
Installation	8
System requirements	8
Installation steps	8
Uninstalling or repairing BitDefender features	9
Introduction	10
How does it work?	10
BitDefender AntiSpam Engine	10
BitDefender AntiVirus Engine	11
Description and Features	12
Description.....	12
Features	12
The Management Console	14
General view	14
Product Registration	16
The AntiVirus Module	17
MS Exchange AntiVirus	17
Integration with MS Exchange.....	17
Advanced scan options	18
AntiVirus Engine	20
Selecting the action on infected messages	20
Setting the Quarantine zone.....	21
Mail Notification	22
NetSend Notification.....	24
Statistics	26
Reports	27
Creating a report file	27
Viewing the report file	27
Real Time Virus Reporting	28

The AntiSpam Module	29
General	29
Setting the spam threshold	30
Selecting the action on spam messages	30
Advanced options	31
Engine	32
Heuristic filter	32
White list / Black list	33
URL filter	35
Keyword filter	36
Creating a new keyword filter rule	37
Statistics	40
Reports	41
Creating a report file	41
Viewing a report file	41
Product Update	42
Best practices	44
Frequently Asked Questions	46
BitDefender Enterprise Manager Integration	48
BitDefender Enterprise Manager Description	48
BitDefender Enterprise Manager Main Features	49
Supported clients	50
System requirements	50
How does BitDefender Enterprise Manager work?	51
BitDefender Server	51
BitDefender Local Manager	51
BitDefender Enterprise Management Console	52
BitDefender Deployment Tool	52
BitDefender Update Server	52
Additional Task Templates	54
Configuring BitDefender for MS Exchange 2003	56
Exchange 2003	56
BitDefender AntiVirus Engine	58
BitDefender AntiSpam Engine	58
BitDefender Update	60
Mail Notification	60
Netsend Notification	61
Real Time Virus Report	61
Retrieving BitDefender status	63

Table of contents

Retrieving a list with all BitDefender products installed	65
Sending a message to clients.....	67
Contact information	69

License and warranty

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

These Terms cover BitDefender Corporate Solutions and Services for Companies licensed to you, including related documentation and any update and upgrade of the applications delivered to you under the purchased license or any related service agreement as defined in the documentation and any copy of these items.

This License Agreement is a legal agreement between you (either an individual or a legal person) and SOFTWIN for use of SOFTWIN's software product identified above, which includes computer software and services, and may include associated media, printed materials, and "online" or electronic documentation (hereafter designated as "BitDefender"), all of which are protected by international copyright laws and international treaties. By installing, copying or using BitDefender, you agree to be bound by the terms of this agreement. If you do not agree to the terms of this agreement, do not install or use BitDefender.

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

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

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

APPLICATION SOFTWARE. You may install and use BitDefender, on as many computers as necessary with the limitation imposed by the total number of licensed users. You may make one additional copy for back-up purpose.

SERVER USER LICENSE. This license applies to BitDefender software that provides network services and can be installed on computers that provide network services. You may install this software on as many computers as necessary within the limitation imposed by the total number of users to which these computers provide network services. This limitation refers to the total number of users that has to be less than or equal to the number of users of the license.

DESKTOP USER LICENSE. This license applies to BitDefender software that can be installed on a single computer and which does not provide network services. Each primary user may install this software on a single computer and may make one

additional copy for backup on a different device. The number of primary users allowed is the number of the users of the license.

TERM OF LICENSE. The license granted hereunder shall commence on the purchasing date of BitDefender and shall expire at the end of the period for which the license is purchased.

UPGRADES. If BitDefender is labeled as an upgrade, you must be properly licensed to use a product identified by SOFTWIN as being eligible for the upgrade in order to use BitDefender. A BitDefender labeled as an upgrade replaces and/or supplements the product that formed the basis for your eligibility for the upgrade. You may use the resulting upgraded product only in accordance with the terms of this License Agreement. If BitDefender is an upgrade of a component of a package of software programs that you licensed as a single product, BitDefender may be used and transferred only as part of that single product package and may not be separated for use by more than the total number of licensed users. The terms and conditions of this license replace and supersede any previous agreements that may have existed between you and SOFTWIN regarding the original product or the resulting upgraded product.

COPYRIGHT. All rights, titles and interest in and to BitDefender and all copyright rights in and to BitDefender (including but not limited to any images, photographs, logos, animations, video, audio, music, text, and "applets" incorporated into BitDefender), the accompanying printed materials, and any copies of BitDefender are owned by SOFTWIN. BitDefender is protected by copyright laws and international treaty provisions. Therefore, you must treat BitDefender like any other copyrighted material. You may not copy the printed materials accompanying BitDefender. You must produce and include all copyright notices in their original form for all copies created irrespective of the media or form in which BitDefender exists. You may not sub-license, rent, sell, lease or share the BitDefender license. You may not reverse engineer, recompile, disassemble, create derivative works, modify, translate, or make any attempt to discover the source code for BitDefender.

LIMITED WARRANTY. SOFTWIN warrants that the media on which BitDefender is distributed is free from defects for a period of thirty days from the date of delivery of BitDefender to you. Your sole remedy for a breach of this warranty will be that SOFTWIN, at its option, may replace the defective media upon receipt of the damaged media, or refund the money you paid for BitDefender. SOFTWIN does not warrant that BitDefender will be uninterrupted or error free or that the errors will be corrected. SOFTWIN does not warrant that BitDefender will meet your requirements.

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

DISCLAIMER OF DAMAGES. Anyone using, testing, or evaluating BitDefender bears all risk to the quality and performance of BitDefender. In no event shall SOFTWIN be

liable for any damages of any kind, including, without limitation, direct or indirect damages arising out of the use, performance, or delivery of BitDefender, even if SOFTWIN has been advised of the existence or possibility of such damages.

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

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

IMPORTANT NOTICE TO USERS. THIS SOFTWARE IS NOT FAULT-TOLERANT AND IS NOT DESIGNED OR INTENDED FOR USE IN ANY HAZARDOUS ENVIRONMENT REQUIRING FAIL-SAFE PERFORMANCE OR OPERATION. THIS SOFTWARE IS NOT FOR USE IN THE OPERATION OF AIRCRAFT NAVIGATION, NUCLEAR FACILITIES, OR COMMUNICATION SYSTEMS, WEAPONS SYSTEMS, DIRECT OR INDIRECT LIFE-SUPPORT SYSTEMS, AIR TRAFFIC CONTROL, OR ANY APPLICATION OR INSTALLATION WHERE FAILURE COULD RESULT IN DEATH, SEVERE PHYSICAL INJURY OR PROPERTY DAMAGE.

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

Prices, costs and fees for use of BitDefender are subject to change without prior notice to you.

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

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

The license will terminate immediately without notice if you are in breach of any of its terms and conditions. You shall not be entitled to a refund from SOFTWIN or any resellers of BitDefender as a result of termination. The terms and conditions concerning confidentiality and restrictions on use shall remain in force even after any termination.

SOFTWIN may revise these Terms at any time and the revised terms shall automatically apply to the corresponding versions of the Software distributed with the revised terms. If any part of these Terms is found void and unenforceable, it will not affect the validity of rest of the Terms, which shall remain valid and enforceable.

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

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

Installation

System requirements

To ensure a proper functioning of the product, before installation, verify that the following system requirements are met:

- ➔ Minimum 20 MB available hard disk space (50 MB Recommended)
- ➔ Windows 2000 SP3 or Windows Server 2003 ; MS Exchange 2003

Installation steps

Locate the setup file and double click it with the mouse. This will launch the wizard, which will guide you through the setup process.



Figure 1

Installation steps:

1. Click **Next** in order to continue or click **Cancel** if you want to quit installation.
2. Please read the **License Agreement**, select **I accept the terms in the License Agreement** and click **Next**. If you do not agree with these terms, select **I do not accept the terms in the License Agreement** and click **Next**. The installation process will be abandoned and you will exit setup.
3. Keep selected **View Readme file** option if you want to see the readme file at the end of the installation process. Click **Install** in order to begin the installation of the product. Click **Back** to go to the previous step or click **Cancel** if you want to abandon the setup process.
4. Click **Finish** to complete the product installation.



You may be asked to restart your system so that the setup wizard can complete the installation process.

Uninstalling or repairing BitDefender features

If you want to repair or uninstall the initial installation of **BitDefender** from the Windows menu select **Start** → **Programs** → **BitDefender for MS Exchange 2003** → **Repair or Uninstall**.

You will be requested to confirm your choice by clicking **Next**. A new window will appear where you can select:

- **Repair** – Re-install all program components installed by the previous setup.
- **Remove** – Remove all installed components.

To continue setup, select one of the two options listed above. Select **Remove** for a clean re-installation.

Introduction

How does it work?

BitDefender for MS Exchange 2003 is the perfect solution BitDefender offers you in order to keep the mail server FREE from viruses & spam. The product is designed and implemented in a modular manner, thus it can easily adapt to any work environment.

The schema below shows the way BitDefender works

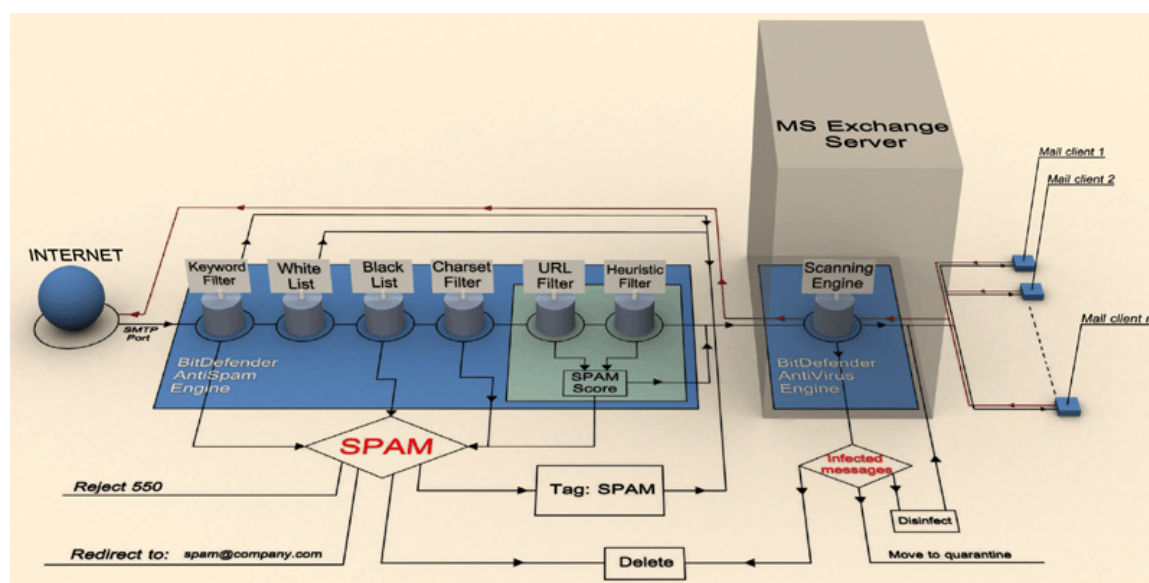


Figure 2

BitDefender for MS Exchange 2003 includes two engines: **BitDefender AntiSpam Engine** and **BitDefender AntiVirus Engine**.

BitDefender AntiSpam Engine

Spam is a growing problem, both for individuals and for organizations. It's not pretty, you wouldn't want your kids to see it, it can get you fired (for wasting too much time or from receiving questionable content in your office mail) and you can't stop people from sending it. The next best to that is, obviously, to stop receiving it. Unfortunately, spam comes in a wide range of shapes and sizes, and there's a lot of it.

The [BitDefender AntiSpam Engine](#) incorporates six different filters: [Keyword filter](#), [White list](#), [Black list](#), [Charset filter](#), [URL filter](#) and [Heuristic filter](#).

Every e-mail that comes from the Internet is first checked with the [Keyword filter](#) filter. It will verify if there is a rule created for this e-mail. If YES the e-mail will be passed to the **BitDefender AntiVirus Engine** or will be tagged as spam (depending on the rule action). If NOT the [White list](#) will take over the e-mail.

If the sender is on the [White list](#) the e-mail will be delivered directly to the mail server. Otherwise the [Black list](#) filter will take over the e-mail to verify if the sender is on the [Black list](#). The e-mail will be tagged as **SPAM** if a match has been made.

If not, the [Charset filter](#) will check if the e-mail is written in Cyrillic or Asian characters. If the server is configured to reject charsets the e-mail will be tagged as **SPAM**. If the e-mail is not written in Asian or Cyrillic it will be passed to the URL filter.

The [URL filter](#) will look for links and it will compare the links found with the links from the BitDefender database. In case of a match +45 will be added to the spam score.

The [Heuristic filter](#) will take over the e-mail and will perform a set of tests on all the message components, (i.e. not only the header but also the message body in either HTML or text format), looking for words, phrases, links or other characteristics of spam. The result is that it will add a spam score to the e-mail.

If the aggregate score (URL score + heuristic score) exceeds the spam score for a message (set by the user in the [MS Exchange AntiSpam](#) section as a threshold score), the message is considered **SPAM**.

The non-spam and the spam tagged messages will be verified further by the **BitDefender AntiVirus Engine**.

BitDefender AntiVirus Engine

The **BitDefender AntiVirus Engine** will check the e-mail for viruses with the BitDefender powerful scanning engines (**ICSA Labs-**, **Checkmark-** and **VB-**certified).

It will identify the viruses contained in the message body or attachment, including RAR, ZIP, ARJ, LZH, LHA, ACE, GZIP, TARGZ, JAR, UUE, MIME or CAB archives, no matter how they were created (self-extractable, multivolume, etc). Depending on the BitDefender actions, the infected messages can be disinfected, deleted or moved to quarantine and alarm messages (by e-mail or through netsend) can be sent to the persons in charge with the administration and the protection of the network.

If the message passes this engine it will be delivered to the e-mail client.

Description and Features

Description

BitDefender for MS Exchange 2003 provides antivirus & antispam protection deeply integrated with the MS Exchange 2003 server. This product embodies the best of BitDefender technologies to create a wholly clean Exchange environment.

Due to the VS-API 2.5 technology, **BitDefender for MS Exchange 2003** seamlessly integrates with the e-mail server, assuring advanced filtering of e-mail messages without affecting server performance or e-mail traffic.

Features

AntiVirus Scanning and Cleaning

Real time scanning of attachments and message bodies, without slowing down e-mail traffic. **BitDefender for MS Exchange 2003** ensures 100% detection rate for all viruses in circulation through its powerful scanning engines from BitDefender Professional, certified by certified by **ICSA Labs**, **Checkmark** and **Virus Bulletin**.

Blocks Infected Messages

Filters and blocks messages if attachment or message body include a virus, Trojan, backdoor or other potentially dangerous active code. Blocks infected files regardless of the archive or compression type.

Scanning at transport level

Messages may be scanned at the transport level using VS-API 2.5. This allows messages passing through a gateway Exchange server that would not normally enter the Exchange store to be scanned. This prevents infected messages from entering the Exchange organization.

Outbound scanning

For sent messages, outbound scanning has been redesigned (in Exchange 2000 SP3 as well as Exchange 2003) such that all outbound messages will be scanned prior to being sent.

Update pushing

BitDefender for MS Exchange 2003 can be configured to initiate an update upon receipt of a specially crafted "update announcement" message from BitDefender Labs (subscription service).

AntiSpam filtering

The existing AntiSpam Infrastructure of Exchange 2003 is leveraged for AntiSpam protection. In addition to that, BitDefender proprietary technologies are used.

Heuristic Analysis Technology

The heuristic filter performs a set of tests on all the message components, (i.e. not only the header but also the message body in either HTML or text format), looking for words, phrases, or links or other characteristics of which are common to spam.

WBL (White List / Black List) Support

This quite simply means that the admin can set a list of trusted and untrusted addresses from which to respectively "always accept" or "always reject" e-mail messages.

Fully Configurable Reactions

- The e-mail messages tagged as spam can be sent to a valid, admin-set address, for periodic checking.
- The score returned by the AntiSpam library can be appended to the e-mail subject line. This is only done to e-mail which exceeds the spam threshold.
- An attribute indicative of confidence level can be added to the header for all the messages (spam or non-spam).
- The e-mail messages tagged as spam can be rejected (SMTP error 550) or dropped.

Detailed Reports and Statistics

BitDefender for MS Exchange 2003 comes with a separate reports module which provides daily, weekly or monthly statistics organized by categories. The reports can be generated and viewed in the administration console.

Intelligent Signature Update

Enables automatic update of virus definitions, without user intervention, directly from the BitDefender servers or from administrator-approved mirror sites. Thus, server traffic protection is kept up-to-date, ensuring swift and effective reaction.

Instant Warning Messages

If a virus is detected, detailed warning messages are sent instantaneously to the network security and management staff.

Remote Management

Enables remote configuration of the server protection, by simply installing the management console on one computer in the network.

Secure Communication

All communication between the management console and the e-mail servers is completely secure, preventing unauthorized actions, which contravene company security policy.

Fully integrated with Enterprise Manager

BitDefender for MS Exchange 2003 is fully compatible with **BitDefender Enterprise Manager**, offering organizations centralized management for antivirus protection and security policies inside complex networks.

24/7 hours professional technical support

Offered by qualified support representatives and an online database with answers to Frequently Asked Questions.

The Management Console

General view

BitDefender for MS Exchange was designed with a centralized management console, which allows the configuration of the protection options for all BitDefender modules. In other words, it is enough to open the management console in order to have access to all modules.

The access to the management console is made through the Windows Start menu, by following the path **Start → Programs → BitDefender for MS Exchange 2003 → BitDefender for MS Exchange 2003**.

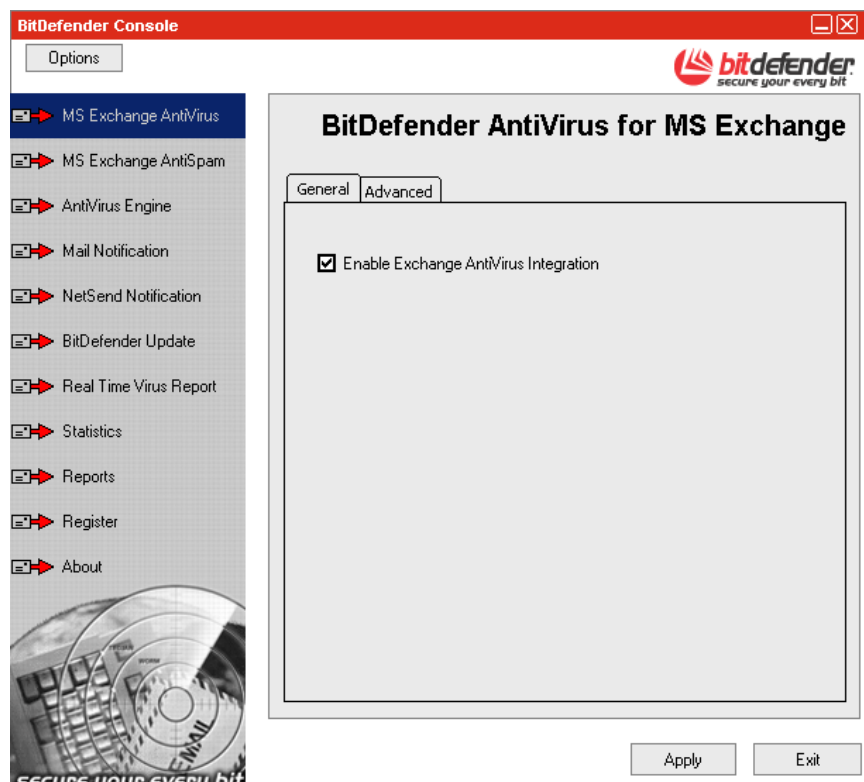


Figure 3

On the left side of the management console you can see the module selector:

- [MS Exchange AntiVirus](#) - to enter the section where you can enable/disable the antivirus protection offered by BitDefender and where you can specify the scan options;
- [MS Exchange AntiSpam](#) – to access the AntiSpam configuration window.
- [AntiVirus Engine](#) – to select the action, in case an infected file is detected, and the location of the quarantine area;

- [Mail Notification](#) – to access the section where you can configure BitDefender to send alarm messages by e-mail, when an unexpected situation appears.
- [NetSend Notification](#) – to access the section where you can configure BitDefender to send alarm messages by netsend, when an unexpected situation appears.
- [BitDefender Update](#) – to access the configuration window for product update;
- [Real Time Virus Report](#) – to access the virus reporting section;
- [Statistics](#) – to see the statistics regarding the [antivirus](#) & [antispam](#) activity;
- [Reports](#) – to see the reports regarding the [antivirus](#) & [antispam](#) activity;
- [Register](#) – to access the section where you can register BitDefender.
- [About](#) – to access the section where can see the contact information and the product details.

The **Options** button can be seen from any section of the product. It will have as effect, the opening of a window that allows you to connect to a remote computer or to change the administrative BitDefender password.



Figure 4

The **Options** menu contains:

- **Connect to a remote computer** - will open a window where you can specify the server's IP and the password.
- **Change administrative password** - will open a window where you can specify the password. Type the password in the field **Password** and confirm it in the field **Confirm**.



You must set a password on the remote computer before you can connect to it.

If you want to open the **Help file** you must follow the path: **Start** → **Programs** → **BitDefender for MS Exchange 2003** → **BitDefender Help**.

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 purchase the product you have to provide a new serial number. To modify the default serial number click **Register** from the management console.

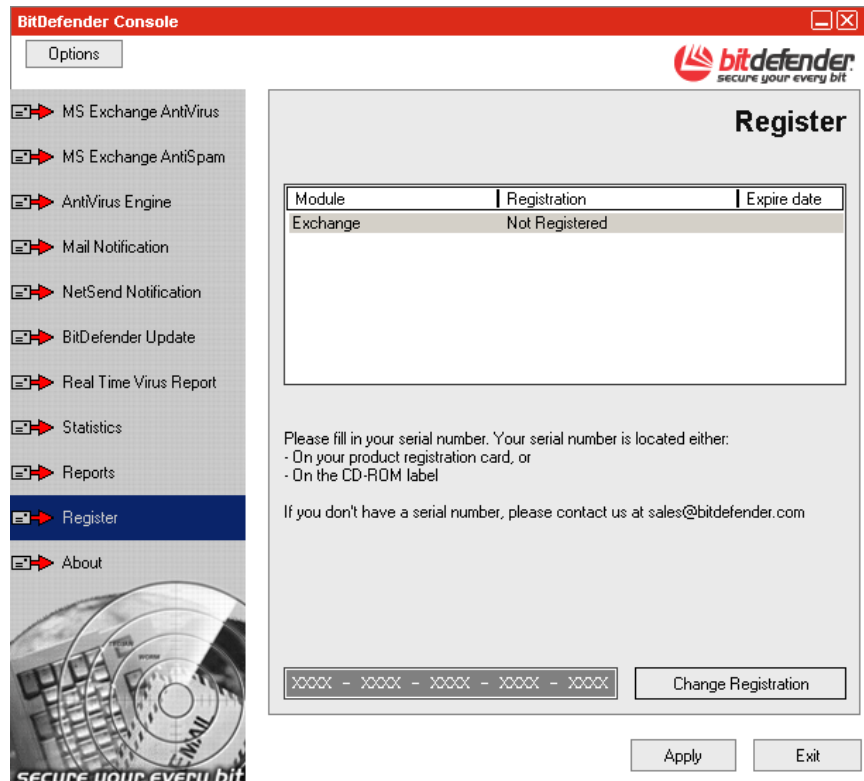


Figure 5

The window offers information about the status of the product (registered or not) and the expiration date.

Steps to follow in order to register the product:

- Select the product from the **Module** pane;
- Type in the serial number in the selected area;
- Click **Change Registration**;
- Click **Apply**.

If the number is valid, the status of the product changes to registered and the expiration date appears.

The AntiVirus Module

In case you haven't already opened the management console, you can access it from the Windows Start menu, following the path **Start → Programs → BitDefender for MS Exchange 2003 → BitDefender for MS Exchange 2003**.

MS Exchange AntiVirus

Integration with MS Exchange

The MS Exchange mail server was designed with a low level interface, VS API, especially designed by Microsoft to offer a support for antivirus scanning and to allow the scan of the multiple recipients messages once, before delivery, instead of many times, for each mail recipient. BitDefender deeply integrates within this interface.

In the management console, click **MS Exchange AntiVirus**.

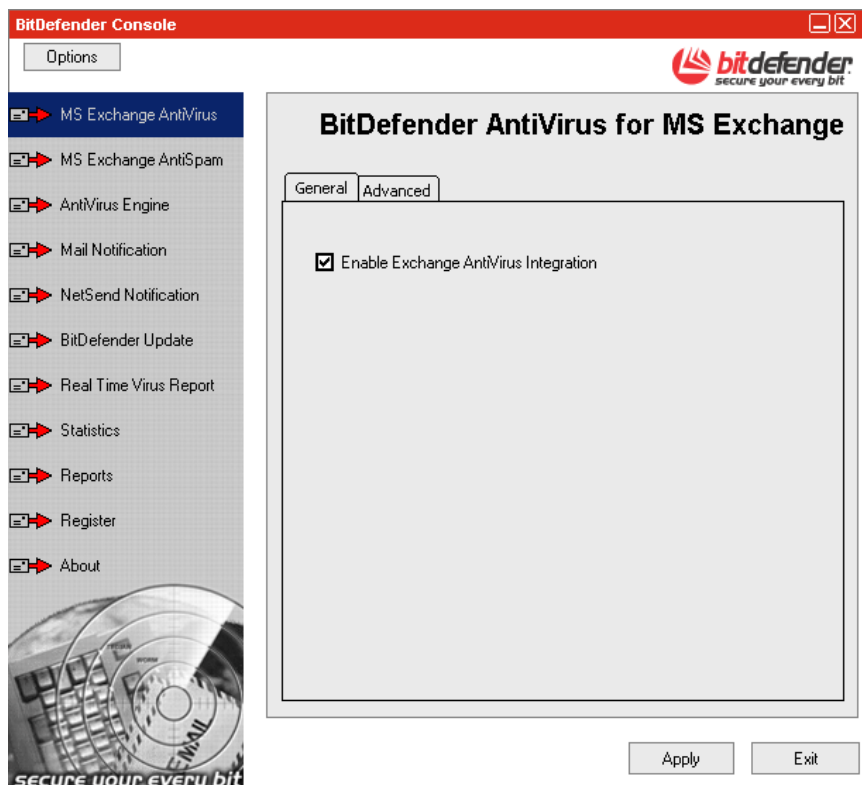


Figure 6

The protection configuration for MS Exchange mail server is very simple. In order to enable the antivirus protection, all you have to do is to select the checkbox corresponding to **Enable Exchange AntiVirus Integration**.

TIP: To enable the antispam protection you must, access the [MS Exchange AntiSpam](#) section and select the checkbox corresponding to **AntiSpam Proxy**.

Click **Apply** in order to save the changes.

Advanced scan options

In order to select the scan options you must click the **Advanced** tab in the **MS Exchange AntiVirus** section. The next window will appear:

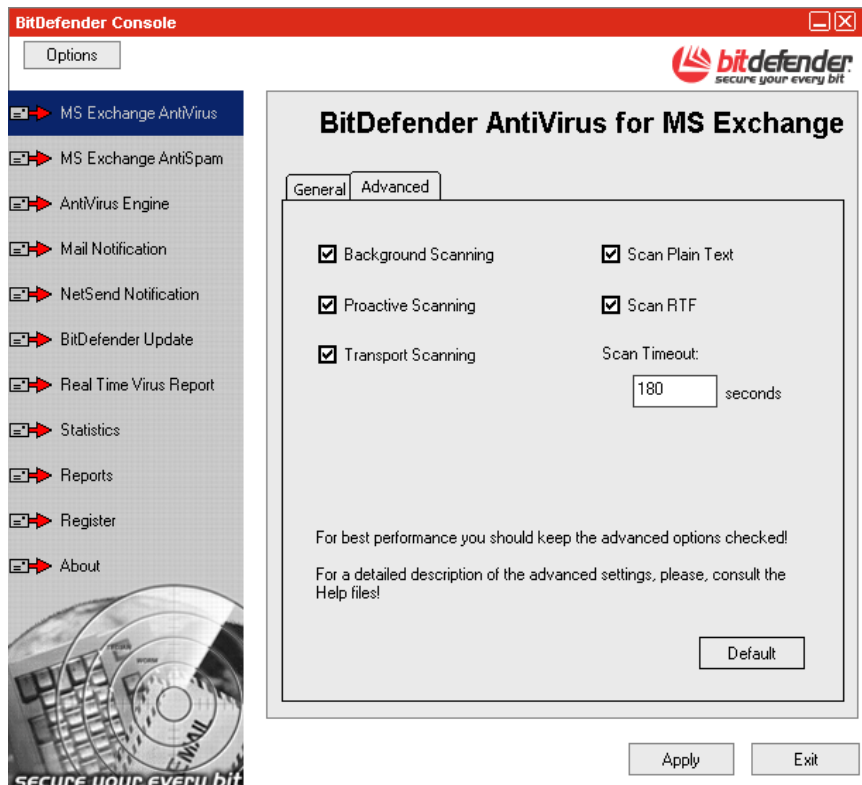


Figure 7

This section contains the following options:

Background Scanning

Means scanning of all folders with a low priority. When an object, that has been checked by background scanning, is requested it will not be scanned again (unless a virus definition update has been made).

The information store will use one thread, per database, running at low priority to perform background scanning of the messages and attachments. Once the background scanning is completed, the thread is terminated. These threads are not part of the global virus-scanning thread pool used for on-access scanning.

Select this option in order to optimize the scanning process.

Proactive Scanning

When a message is submitted to the information store, either via a client or a transport agent, it is placed in the global scanning queue with a low priority. If and when there are threads available in the thread pool and no high priority item remains to be scanned, each item with the low priority is submitted for scanning.

If an item is in the low priority list and a client attempts to access the message, the item will be reprioritized and marked with high priority. It will also be removed from the low priority list. If this setting is disabled, and messages were not submitted for scanning for any reason, they will be scanned when they are accessed.

Transport Scanning

Messages may be scanned at the transport level using this option. This prevents infected messages from entering the Exchange organization.

Messages are submitted to the Exchange store from the transport engine, allowing access to messages via the VSAPI. Following scanning, messages are resubmitted to transport for delivery to their destination. Any message scanned at the gateway will be rescanned on the back-end server. The transport scanning functionality is not activated by default.

Scanning Plain Text

Select this option in order to scan body messages in plain text format.

Scanning RTF

Select this option in order to scan body messages in RTF (Rich Text Format) format.

Scanning Timeout

You may introduce here the maximum time allocated for scanning an object. If the scanning process is not completed before the time out, an error is returned and the access to the un-scanned object is prohibited.

At the end, click **Apply** in order to save the changes.

AntiVirus Engine

In the management console, click **AntiVirus Engine**.

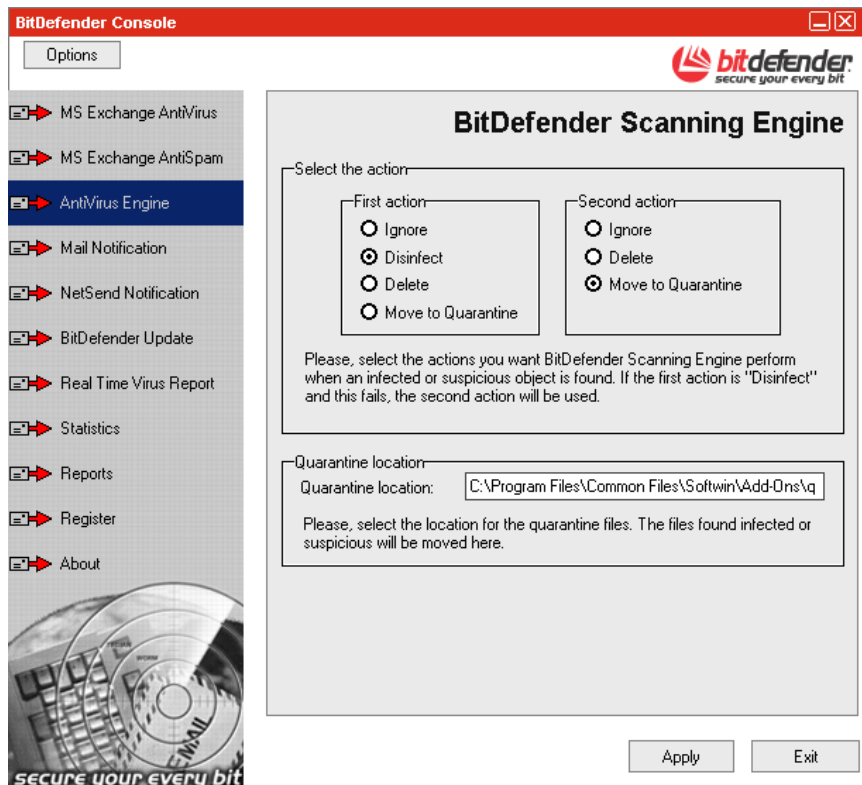


Figure 8

Selecting the action on infected messages

BitDefender allows selecting two actions in case an infected message is found. The second action is enabled only in case the first action you selected is to disinfect the infected messages.

You can select one of the following actions:

First Action	Description
Ignore	The infections found are ignored and the messages will be delivered to the mail recipients, along with the infected part*, without any reaction.
Disinfect	The infected part* of the message will be disinfected. If the disinfection fails, a second action will be taken.
Delete	The infected part* of the message will be deleted. A <code>virus info.txt</code> will be delivered to the mail recipient informing him about the infection and the action BitDefender took.
Move to quarantine	The infected file will be isolated in the quarantine zone.

Second Action	Description
Ignore	In case the disinfection of the message fails, this is delivered to the mail recipient without any change and still containing the infection.
Delete	If the disinfection fails, the infected part* will be deleted. A <code>virus info.txt</code> will be delivered to the mail recipient informing him about the infection and the action BitDefender took.
Move to quarantine	If the disinfection fails, the infected part* will be moved to the quarantine folder. A <code>virus info.txt</code> will be delivered to the mail recipient informing him about the infection and the action BitDefender took.

* the body or the attachment(s) of the messages

TIP: We recommend using 1st action: **Disinfect**, 2nd action: **Delete**.

Setting the Quarantine zone

The default location of the quarantine zone is: `C:\Program Files\Common Files\Softwin\ADD-ONS\quar`. If you want to change it, type in the complete path in the **Quarantine location** field.

Click **Apply** to save the changes.

Mail Notification

If an unexpected situation appears, there is the possibility of sending alarm messages by e-mail. To setup this service, click **Mail Notification**.

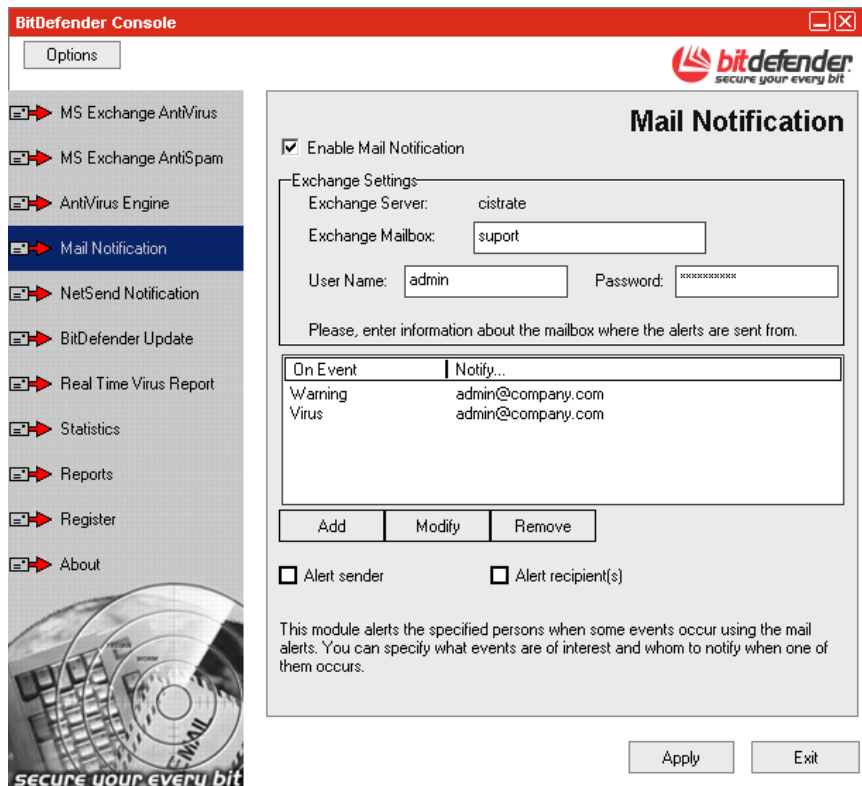


Figure 9

Select the **Enable Mail Notification** check box in order to activate the service.

Types of events that can generate alarm messages:

Event	Description
Warning	Generates a warning message in case a special situation appears. Such as: license expiration (BitDefender will alert you three days before it expires), protection disabled and so on.
Error	Generates a message that announces the apparition of a malfunction of BitDefender. Such situations may occur, for example, because of the accidental deletion of some files or failure to load the AntiSpam engines.
Virus	A message is generated in case an infected or suspicious file is detected.

In order to send alerts via e-mail you must first specify some information in the section **Exchange Settings**:

- ➔ **Exchange mailbox** - type in the name of the mailbox you use to send alerts.
- ➔ **User name** - type in the user name.



The user must have rights on the specified mailbox.

→ **Password** - type in the administration password.

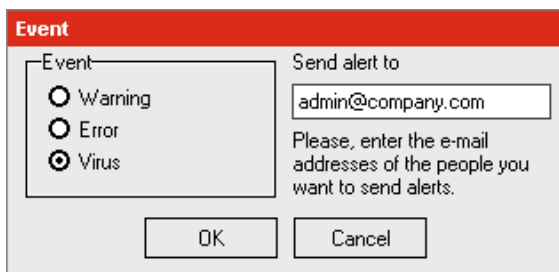
 **Note**

It is necessary to type in a valid e-mail address for the Mail server, otherwise the server may decline sending an e-mail whose sender (e-mail address) is unknown to him.

The section contains 3 buttons:

- **Add** - to add a new e-mail address where an alert will be sent when an exceptional situation appears.
- **Modify** - to modify the recipient that will be warned or the event that causes the warning.
- **Remove** - to delete a warning event.

If you wish to create an event that generates alerts via e-mail, click **Add**. In the window that appears select the event's type, by simply clicking it and type in the e-mail address(es) where the alert will be delivered.



Click **Ok** to save the event or click **Cancel** to abandon.

Figure 10

TIP: If you want to send messages to more than just one e-mail recipient, these addresses must be separated by commas.

If you want to change an event (the e-mail recipient or the event type), click **Modify**. Select a new type of event, or specify a new e-mail address. Click **Ok** if you want to save the changes or click **Cancel** if you want to keep the previous settings.

 **Note**

To modify or delete an event it is necessary to select it and then click **Modify** or **Remove**. If you click **Remove**, the event will be removed without further warning.

Select the check box corresponding to **Alert sender** / **Alert recipient(s)** if you want to notify the sender / the receiver(s) when a virus is found.

Click **Apply** to save the changes.

NetSend Notification

If an unexpected situation appears, there is the possibility of sending alarm messages by netsend. To setup this service, click **NetSend Notification**.

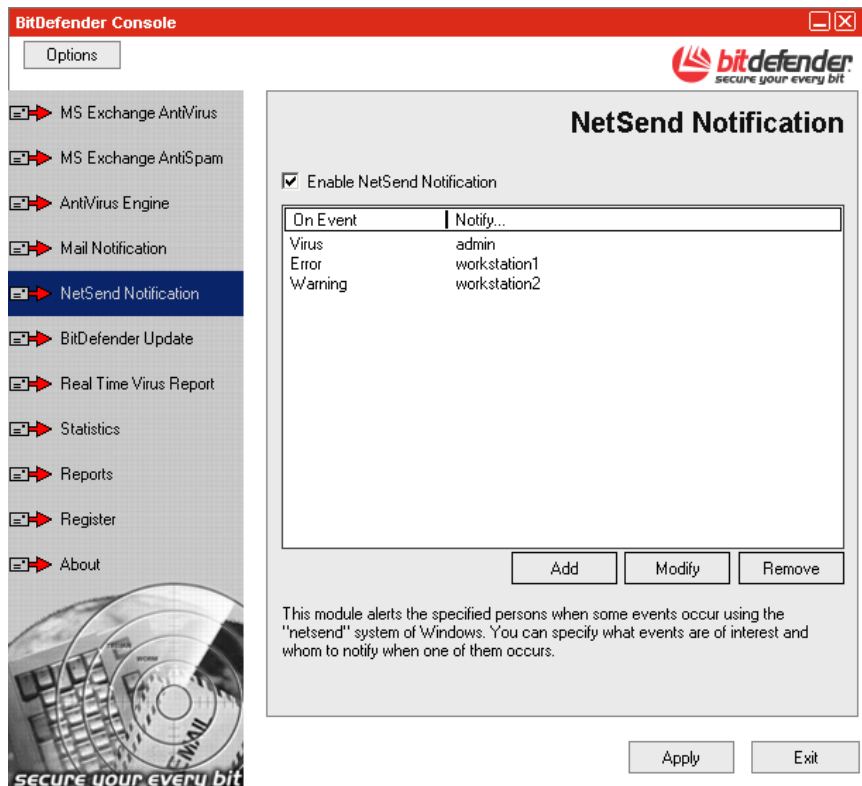


Figure 11

Select the **Enable NetSend Notification** check box in order to activate the service.

There are many types of events that can generate alarm messages:

Event	Description
Warning	Generates a warning message in case a special situation appears. Such as: license expiration (BitDefender will alert you three days before it expires), protection disabled and so on.
Error	Generates a message that announces the apparition of a malfunction of BitDefender. Such situations may occur, for example, because of the accidental deletion of some files or failure to load the AntiSpam engines.
Virus	A message is generated in case an infected or suspicious file is detected.

The section contains 3 buttons:

- ➔ **Add** - to add a new workstation where an alert through netsend will be sent when an exceptional situation appears.
- ➔ **Modify** - to modify the workstation who will be warned or the event that causes the alert.
- ➔ **Remove** - to delete a warning event.

If you wish to create an event that generates alerts via netsend, click **Add**. In the window that appears select the event's type, by simply clicking it and type in the recipient where the alert message(s) will be sent.



Click **Ok** to save the event or click **Cancel** to abandon.

Figure 12

TIP: If you want to send messages to more than just one workstation, these must be separated by commas.

If you want to modify a previously created event, select it and click **Modify**. A window with the settings for that event will open. Select a new type of event or type in the **Send alert to** field the name of another workstation.

Click **Ok** if you wish to save the changes or **Cancel** if you wish to abandon and keep the previous options.



Note

To modify or delete an event it is necessary to select it and then click **Modify** or **Remove**. If you click **Remove**, the event will be removed without further warning.

Click **Apply** in order to save the changes.

Statistics

To see the statistics regarding the antivirus activity, in the **Statistics** section click the **AntiVirus** tab placed at the top of the window.

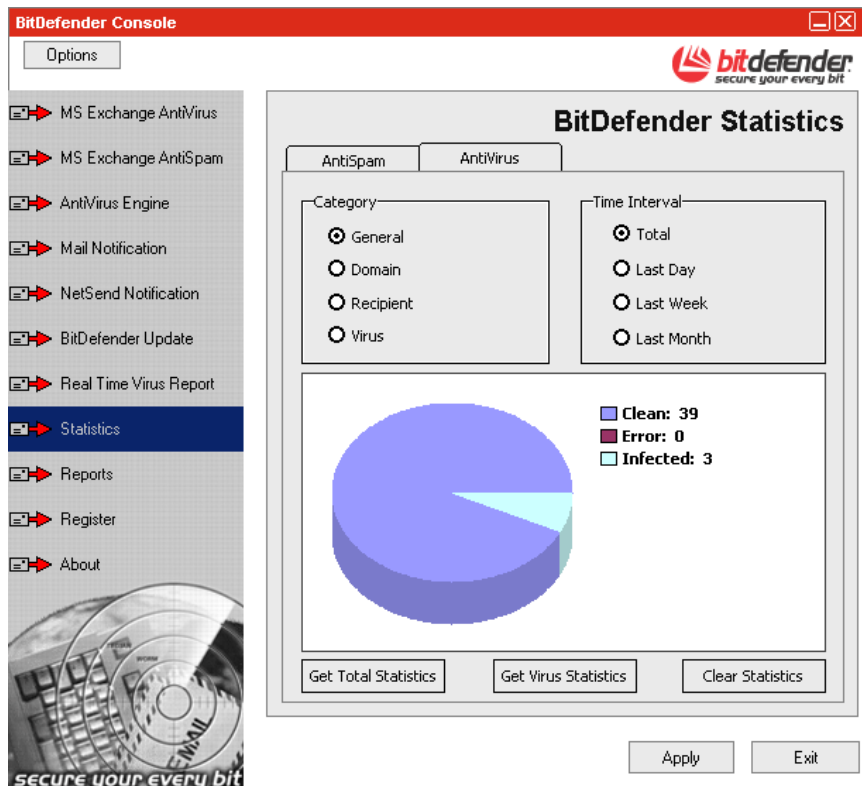


Figure 13

Use the management console to create statistics concerning the antivirus activity. To create statistics, you must select:

- ➔ The category (**General, Domain, Recipient or Virus**);
- ➔ The time interval (**Total, Last Day, Last Week or Last Month**).

After selecting those you may click the **Get Total Statistics** button (to view the statistics regarding the mail activity) or click the **Get Virus Statistics** button (to view the statistics regarding the virus activity).

Reports

To see the reports regarding the antivirus activity, in the **Reports** section click the **AntiVirus** tab placed at the top of the window

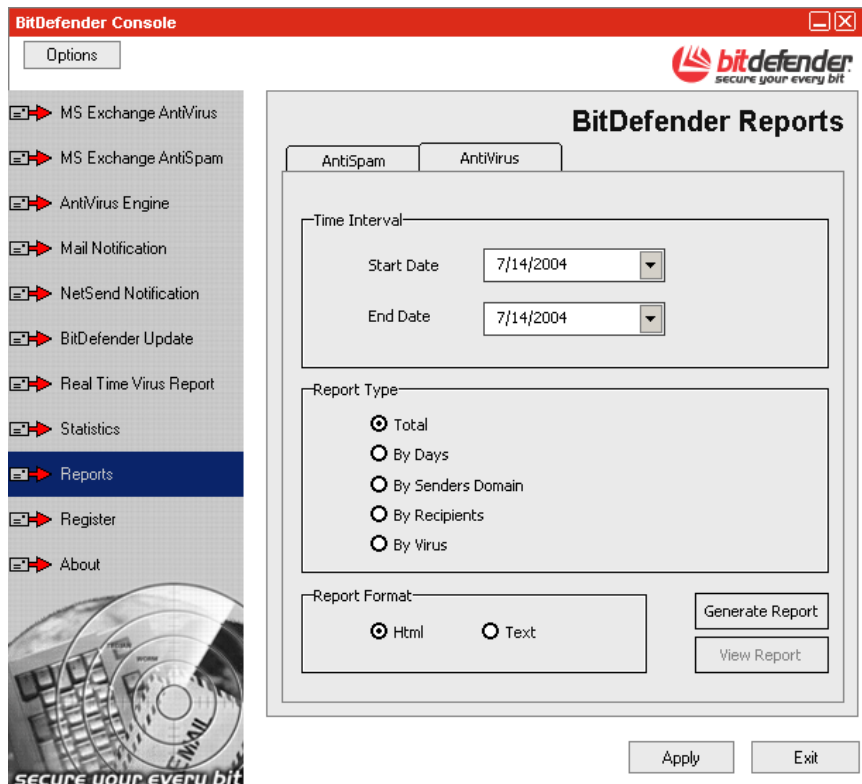


Figure 14

Here you can generate report files and you can see them.

Creating a report file

To create a report file, you must select:

- The time interval;
- The report type (**Total**, **By Days**, **By Senders Domain**, **By Recipients** or **By Virus**);
- The report format (**Html** or **Text**).

After selecting those you may click **Generate Report**. The new reports are located in `program files\common files\softwin\reports`

Viewing the report file

The information contained in a report file can be seen by clicking the **View Report** button. You can view: the number of the infected messages, the number of all the messages and the number of errors (when BitDefender failed to analyze the message).

Real Time Virus Reporting

This feature is customized on countries and allows sending alerts about the detected viruses to the BitDefender Lab. The reports will contain no confidential data, such as your name, IP address or others, and will not be used for commercial purposes. The information supplied will contain only the name of the country and the virus name and will be used solely to create statistic reports.

Click **Real Time Virus Report** from the management console.

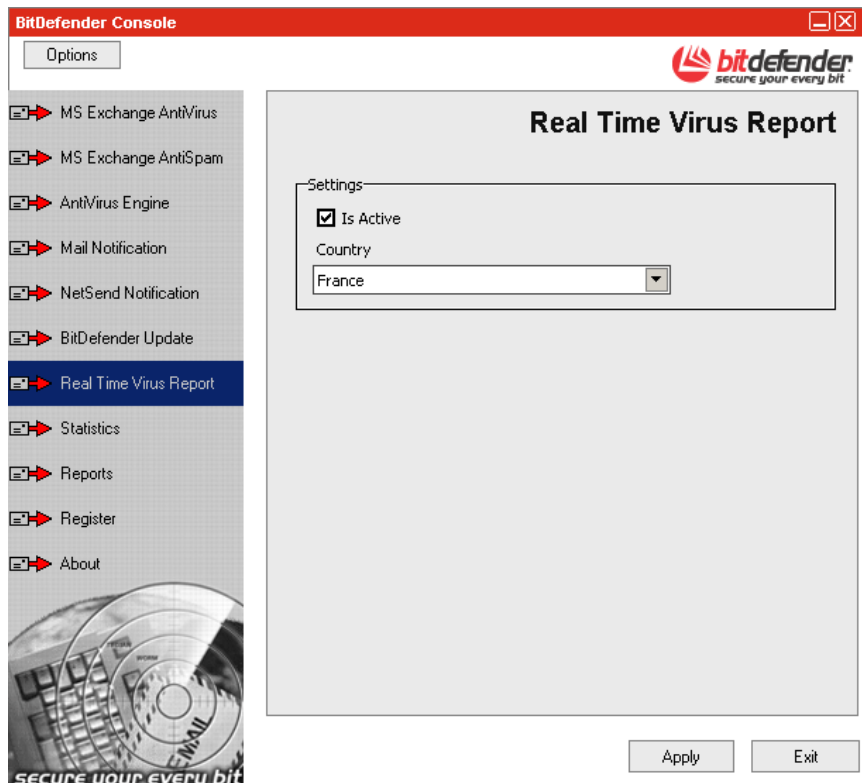


Figure 15

Select the check box corresponding to **Is Active** in order to activate the virus reporting, then, from the scroll down list, select the country where you live. If you want to stop the virus reporting, unselect this option.

Click **Apply** to save the changes.

The AntiSpam Module

In case you haven't already opened the management console, you can access it from the Windows Start menu, following the path **Start → Programs → BitDefender for MS Exchange 2003 → BitDefender for MS Exchange 2003**.

The AntiSpam module has 4 panes: **General**, **Advanced**, **Engine** and **Keyword Filter**.

- [General](#) – to access the AntiSpam configuration window.
- [Advanced](#) – to access the section where you can set BitDefender to check for authenticated connections .
- [Engine](#) – to access the section where you can enable / disable the heuristic filter, the White / Black lists and the URL filter. You can also configure them.
- [Keyword Filter](#) – to access section where you can create content filtering rules.

In the management console, click **MS Exchange AntiSpam**.

General

The **MS Exchange AntiSpam** section opens default in the **General** section.

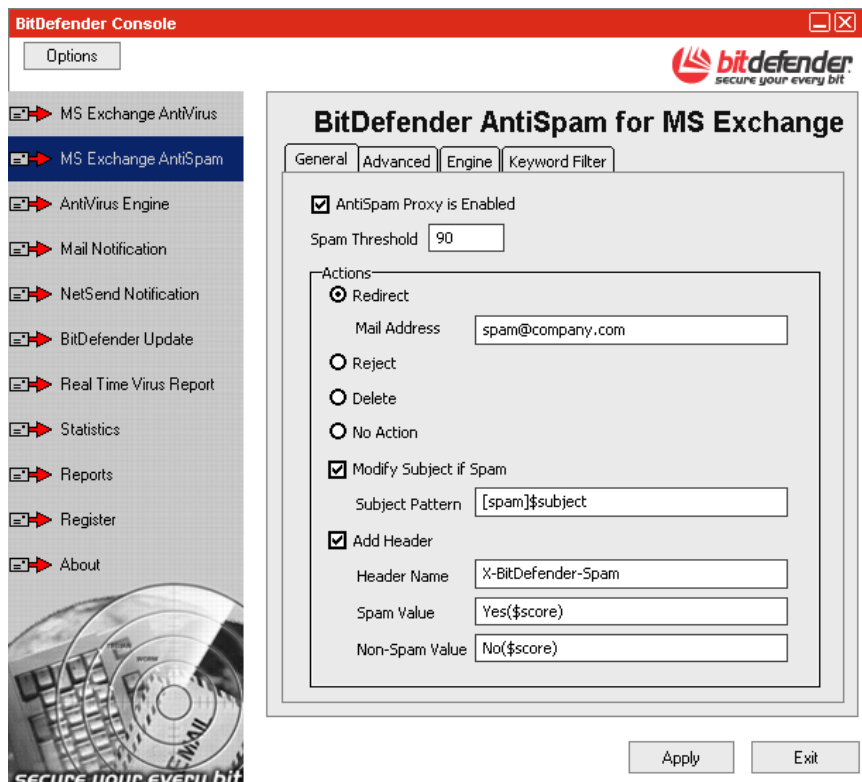


Figure 16

In this section you can enable / disable BitDefender AntiSpam, you can select the action to be taken on messages (not only the spam messages) and you can set the spam threshold.

TIP: Keep the **AntiSpam Proxy** check box selected to be protected against spam.

Setting the spam threshold

BitDefender checks all the message components against many rules, (i.e. not only the header but also the message body in either HTML or text format), using the **URL filter** and the **Heuristic filter**.

Each rule is given a numerical value and the aggregate of these values is an overall spam score that ranges from 0-100. The overall spam score is measured against the desired level of spam sensitivity (threshold), and a decision is made whether the message is spam or is valid.


If the spam score for a message exceeds the threshold level, the message is considered spam. Exceptions are made if the sender is in the **IPMatch** or **Keyword Filter** tables (as not spam) or on the **White list**.



The default **Spam Threshold** is 90. If you increase this value the filter will let some spam through. If you reduce this value very little spam will pass, but some legitimate messages may be tagged as spam.

Selecting the action on spam messages

BitDefender allows the selection of one of the following actions:

Action	Description
Redirect	<p>The result is that the spam messages are redirected to a specified e-mail address. Select Redirect check box and type the address where spam will be delivered in the Mail Address field. You can type a local e-mail address or one from another SMTP server.</p> <p> You must specify only one address. If the Mail Address field is empty or the e-mail address is invalid the spam messages will not be redirected.</p>
Reject	The result is that the spam messages are rejected with a 550 SMTP error code.
Delete	The result is that the spam messages are deleted.
No Action	The result is that the spam messages will be delivered to the e-mail recipients without any reaction.
Modify Subject if Spam	<p>The result is that the subject of the spam messages will be modified. Select Modify Subject if Spam check box and introduce the desired subject in the Subject Pattern field.</p> <p>The subject must be specified like:</p> <ul style="list-style-type: none"> • <code>[SPAM]</code> - all e-mail messages considered spam will have the subject <code>[SPAM]</code>; • <code>[SPAM]\$\$subject</code> - all e-mail messages considered spam will have the subject: <code>SPAM</code> followed by the original subject - this is default; • <code>[\$score% SPAM]\$\$subject</code> - all e-mail messages considered spam will have the subject: <code>[x% SPAM]</code> followed by the original subject (where <code>x</code> - represents the spam score). <p>For example we have a spam message with the original subject line <code>Very important!</code>. The subject line will be changed to <code>[SPAM]</code> for the first case, <code>[SPAM] Very important!</code> for the second case and <code>[x% SPAM] Very important!</code> for the third case (where <code>x</code> - represents the spam score).</p>

Action	Description
Add Header	<p>The result is that the header of all the messages (spam or not) will be modified. Select the Add Header check box and type the desired header in the Header Name field.</p> <p>The default case is <code>X-BitDefender-Spam</code> as header, <code>Yes(\$score)</code> as spam value and <code>No(\$score)</code> as non-spam value. When a spam is detected the header will be <code>X-BitDefender-Spam: Yes(x%)</code> (where <code>x</code> - represents the spam score). All non-spam messages will have as header <code>X-BitDefender-Spam: No(x%)</code> (where <code>x</code> - represents the spam score).</p>

When you finish, click **Apply** in order to save the changes.

Advanced options

In the **MS Exchange AntiSpam** section click the **Advanced** tab. The next window will appear:

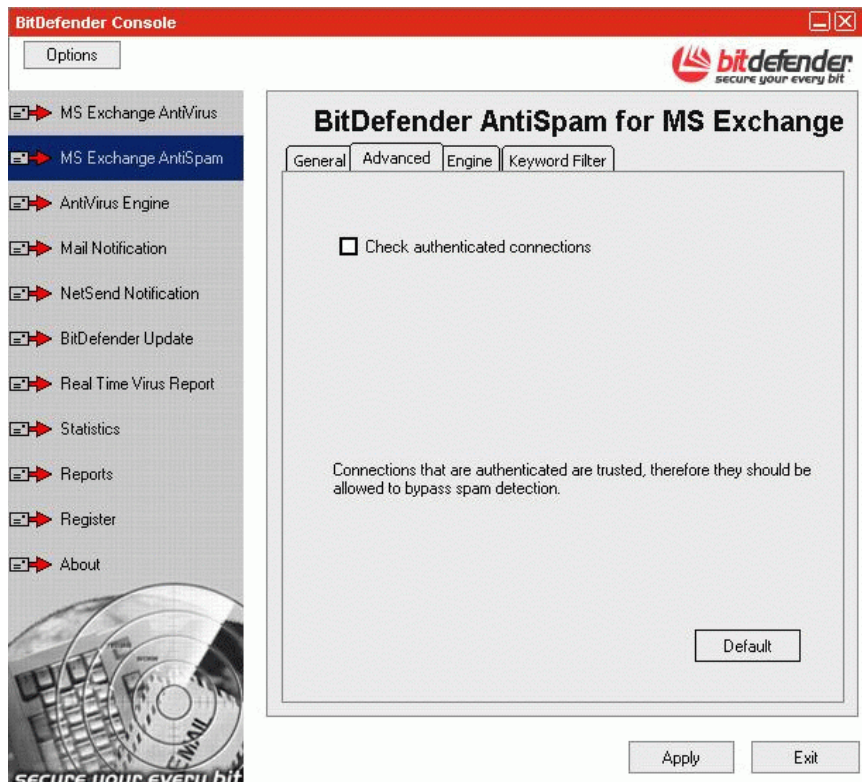


Figure 17

Connections that are authenticated are trusted, therefore they should be allowed to bypass spam detection. The **BitDefender AntiSpam Engine** should only be activated for messages that have been submitted anonymously or are not on a safe connection list.

If you select the check box corresponding to **Check authenticated connection** all the messages will be scanned by the **BitDefender AntiSpam Engine**

Click **Apply** in order to save the changes.

Engine

In the **MS Exchange AntiSpam** section click the **Engine** tab. The next window will appear:

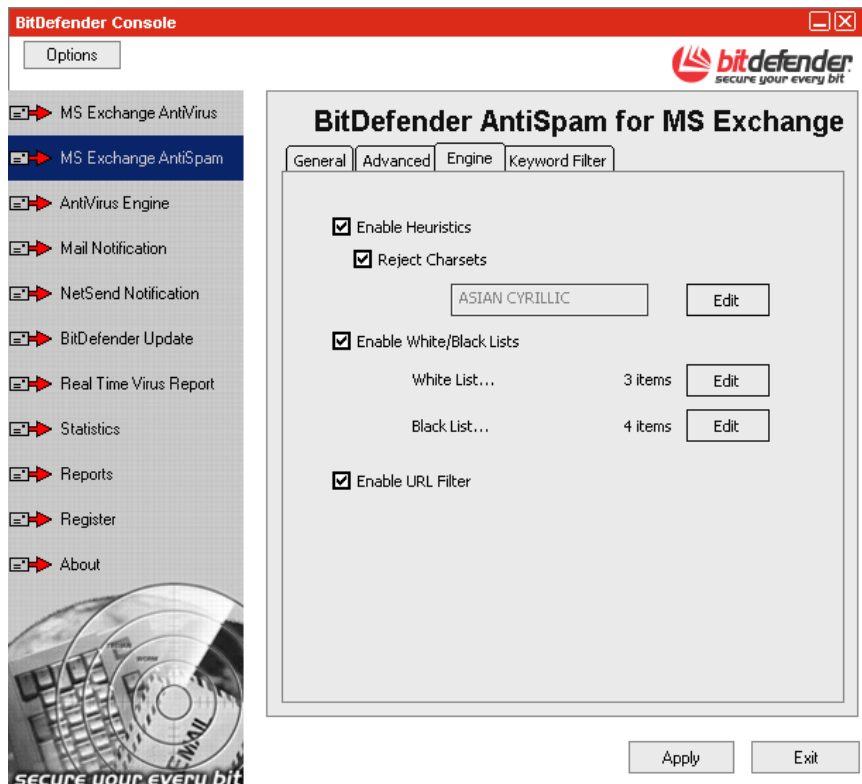


Figure 18

In this section you can enable / disable the heuristic filter, the White / Black lists and the URL filter. You can also configure the charset filter and the White / Black lists.

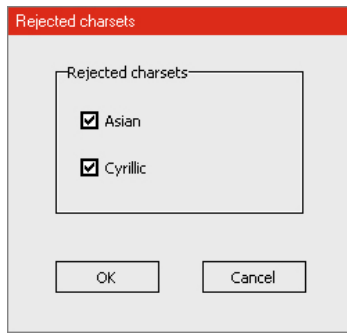
Heuristic filter

The heuristic filter performs a set of tests on all the message components, (i.e. not only the header but also the message body in either HTML or text format), looking for words, phrases, links or other characteristics of spam.

Select the **Enable Heuristics** check box in order to enable the heuristic filter.

! Every time you perform an [update](#) new rules will be added to the heuristic filter; this will help increase the effectiveness of your AntiSpam engine.

The **Reject charsets** option will cause all the e-mail messages written in Cyrillic and / or Asian charsets to be rejected. Select **Reject charsets** check box and click **Edit**. The following window will appear:




Select **Asian** and / or **Cyrillic** check box(es) and click **OK**. E-mails written in **Asian** and / or **Cyrillic** will be considered spam.

Figure 19

White list / Black list

Most people communicate regularly to a group of people or even receive messages from companies or organizations in the same domain. By using **White/Black lists**, the admin can set a list of trusted and un-trusted addresses from which to respectively "always accept" or "always reject" e-mail messages.

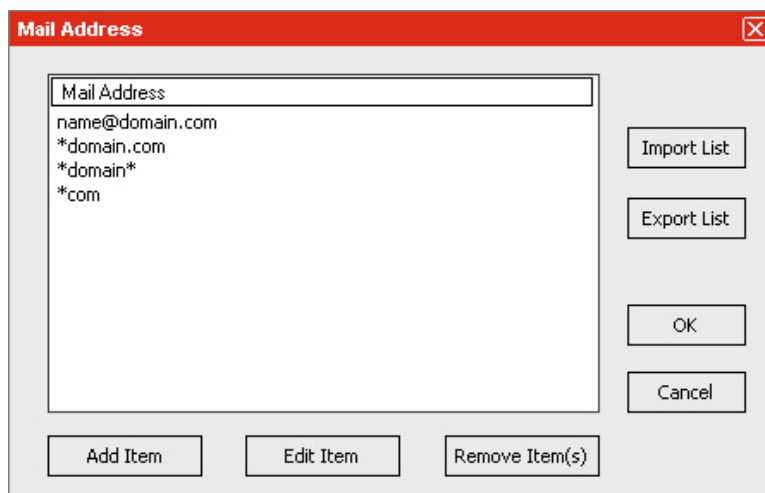
We recommend that you add the trusted addresses to the **White List**. **BitDefender** does not block messages from those on the list; therefore, adding them helps ensure that legitimate messages get through.

 If you wish to re-install the product we recommend you to export the **White/Black Lists** so that you can import them later.

Select **Enable White/Black Lists** check box in order to enable the **White/Black Lists** filter.

White list

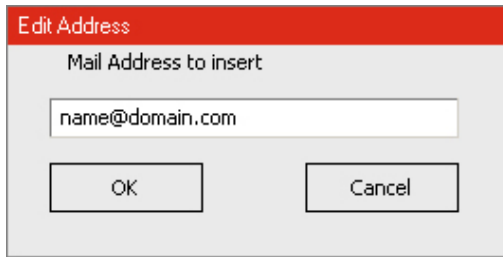
Click **Edit** corresponding to the **White List**. The following window will appear:



Here you can add, modify and remove addresses or you can import or export lists of addresses.

Figure 20

To add an address, click the **Add Item** button. The next window will appear:



Type in the address and click **OK**.

The address must be specified like:
name@domain.com.

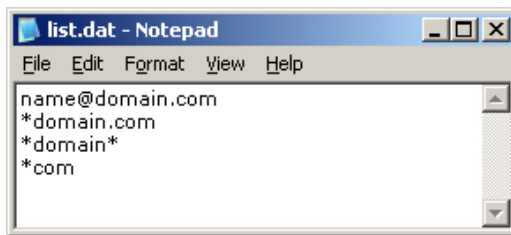
Figure 21

If you want to add a domain you must specify it like this:

- `*@domain.com` OR `*domain.com` - all e-mail messages coming from `domain.com` will be delivered regardless of content;
- `*domain*` - all e-mail messages coming from `domain` (no matter the domain suffixes) will be delivered regardless of content;
- `*com` - all e-mail messages having the domain suffix `com` will be delivered regardless of content.

To delete an item, select it and click the **Remove Item** button. You can select as many items as you want holding SHIFT or CTRL. To modify an item, select it and click the **Edit Item** button.

The **Export List** button is used to save the list to a desired location. The file will have `.dat` as extension and it will look like this:



The addresses are one on a line.



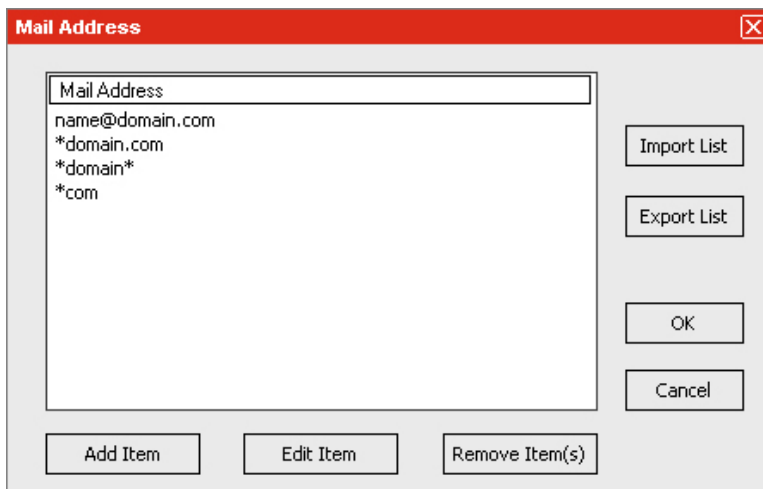
You can edit and write this list and then you can import it by clicking the **Import List** button.

Figure 22

Click **OK** to save and close the **White List**.

Black list

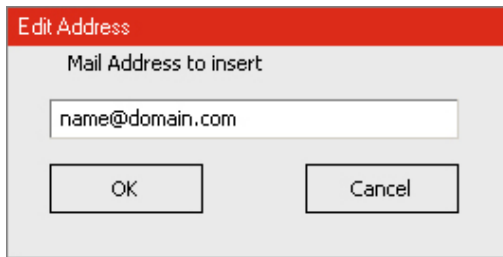
Click **Edit** corresponding to the **Black List**. The following window will appear:



Here you can add, modify and remove addresses or you can import or export lists of addresses.

Figure 23

To add an address, click the **Add Item** button. The next window will appear:



Type in the address and click **OK**.

The address must be specified like:
name@domain.com.

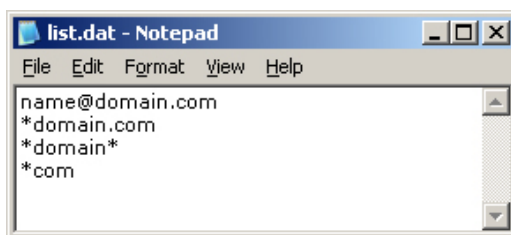
Figure 24

If you want to add a domain you must specify it like this:

- *@domain.com or *domain.com - all e-mail messages coming from domain.com will be tagged as spam;
- *domain* - all e-mail messages coming from domain (no matter the domain suffixes) will be tagged as spam;
- *.com - all e-mail messages having the domain suffix com will be tagged as spam.

To delete an item, select it and click the **Remove Item** button. You can select as many items as you want holding SHIFT or CTRL. To modify an item, select it and click the **Edit Item** button.

The **Export List** button is used to save the list to a desired location. The file will have .dat as extension and it will look like this:



The addresses are one on a line.



You can edit and write this list and then you can import it by clicking the **Import List** button.

Figure 25

Click **OK** to save and close the **Black List**.

URL filter

Most of the spam messages contain links to various web locations (which contain more advertising and the possibility to buy things, usually). BitDefender has a database, which contains links to these kinds of sites.

Every time you perform an [update](#) new links will be added to the URL filter; this will help increase the effectiveness of your AntiSpam engine.

Every URL link in an e-mail will be checked against the URL database. If it will be found, +45 will be added to the spam score.

Select **Enable URL Filter** check box in order to enable the **URL Filter**.

At the end, click **Apply** in order to save the changes.

Keyword filter

In the **MS Exchange AntiSpam** section click the **Keyword filter** tab. The next window will appear:

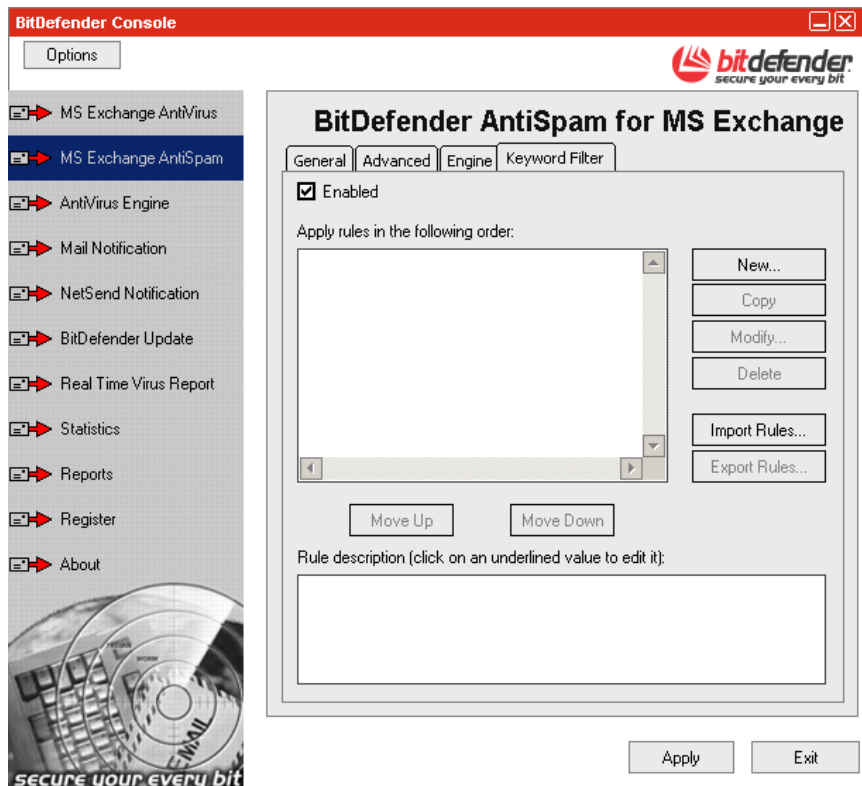


Figure 26

The section contains a list with all the defined rules ordered by their priorities in a descending order. There is also a field that contains the description of the rule, which appears when the rule is selected.

You can always activate/deactivate a rule directly from the list, by selecting/unselecting the corresponding check box.

If you select a rule you can:

- **Multiply it** – click **Copy**. A new rule named **copy of ...** will appear. Multiplying a rule is recommended in case you want to create a new rule by modifying an old one.
- **Modify it** – click **Modify**. The rules wizard will be launched. Follow the same steps as in the case of creating a new rule.
- **Delete it** – click **Delete**. The rule will be erased without further warning.
- **Import / Export it** – click **Import rules/Export rules**. Importing a rule means to load a rule saved on the disk as `.rwz` file. Exporting a rule means saving a rule on the disk as `.rwz` file. You can import/export all the rules by clicking **Import rules/Export rules**.
- **Change its priority** – click **Move up** and **Move down** to grant a higher/lower priority.

Creating a new keyword filter rule

To create a new keyword filter rule, click **New**. This will launch the rule wizard that will guide you through the process.

First step

Type in a name for the rule in the field **Name of the rule** and select at least one condition.

You can observe that in the rule description area, a link, "specific words" or "specific addresses" (depending on the selected condition), appears.

Click it in order to specify the words or the address.

Figure 27

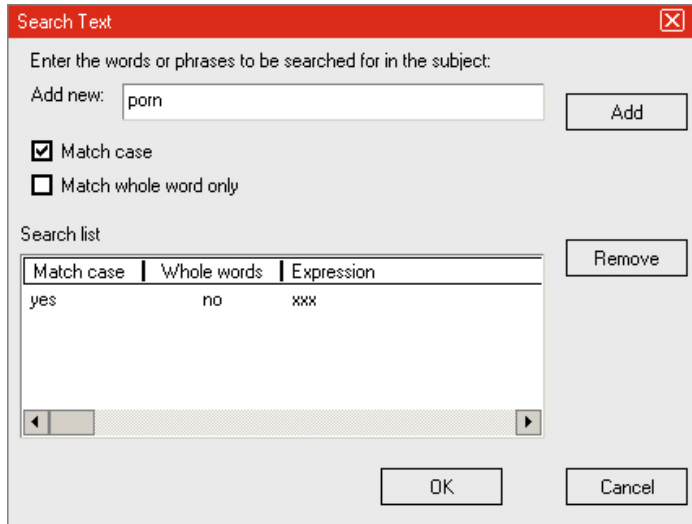
BitDefender contains a collection of elementary predefined rules, with which, depending on the necessities, you can create complex rules. All these rules are described in the table below:

Rule	Description
With "specific words" in subject	The words defined by the administrator are searched in the subject of the message.
With "specific words" in header	BitDefender searches, in the message's header, for the words defined by the administrator.
With "specific words" in the To field	Check if the words specified by the administrator appear in the <code>To</code> field.
With "specific words" in the Cc field	Check if the words specified by the administrator appear in the <code>Cc</code> field.
With "specific words" in the receiver's address	Check if the words specified by the administrator appear in the receiver's address.
With "specific addresses" in the To field	Check if certain addresses appear in the <code>To</code> field.
With "specific addresses" in the Cc field	Check if certain addresses appear in the <code>Cc</code> field.
Send to "specific addresses"	Check if the message has been sent to certain specified addresses.
That has as subject "specific words"	Check if the messages have as subject the words specified by the administrator.

To continue you must click "specific words" or "specific addresses" from the **Rules description** window.

Second step

For rules with "specific words" the following window will appear where you can specify the words.



Type in the specific word in the field **Add new**.

Select **Match case** if you want the checking to be done by matching the case or select the option **Match whole word only**, to check for whole words only.

Click **Add** to add the word to the list.


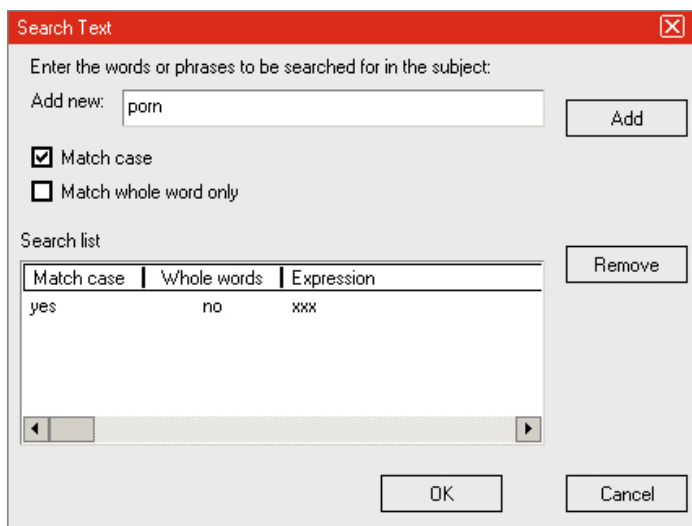
 You can add as many words as necessary.

Figure 28

To delete a word from the list, you must first select it and then click **Remove**.


After making all the required changes, click **Ok**.

For rules with "specific addresses" the following window will appear where you can specify the addresses:



Type in the specific address in the field **Add new**.

Click **Add** to add the word to the list.

 You can add as many addresses as necessary.

To delete an address from the list, you must first select it and then click **Remove**.

Figure 29

After making all the required operations, click **Ok**.

Third step

Now you can see instead of "specific words" / "specific addresses" the word(s) / address(es) you just introduced. Click this link if you want to make any changes.

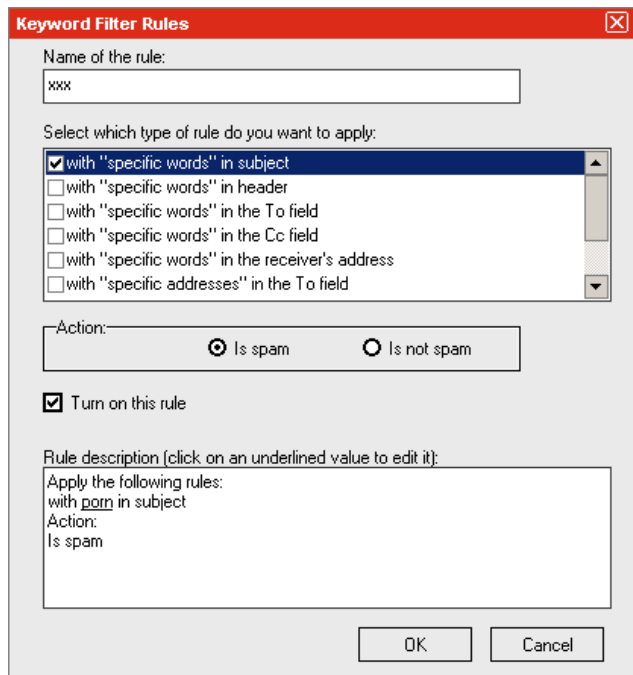


Figure 30

You must select the action for the rule: **Is spam** or **Is not spam**. Select the check box corresponding to the desired one.

Select the option **Turn on this rule** in order to enable the rule.

Click **OK**. The wizard will close and the new rule will appear in the rules list from the [Keyword Filter](#) section.

 **Note**

1. Each message will be verified. The order of the rules is very important, as it sets their priority degree. Thus, a message will be treated conforming to the action of the first rule it applies to. If a message doesn't apply to any of the defined rules, no action will be taken.
2. Defining a very large number of very complex rules can affect the e-mail delivery speed.

At the end, click **Apply** in order to save the changes.

Statistics

To see the statistics regarding the antispam activity click **Statistics** from the management console. The section opens default in the **AntiSpam** pane.

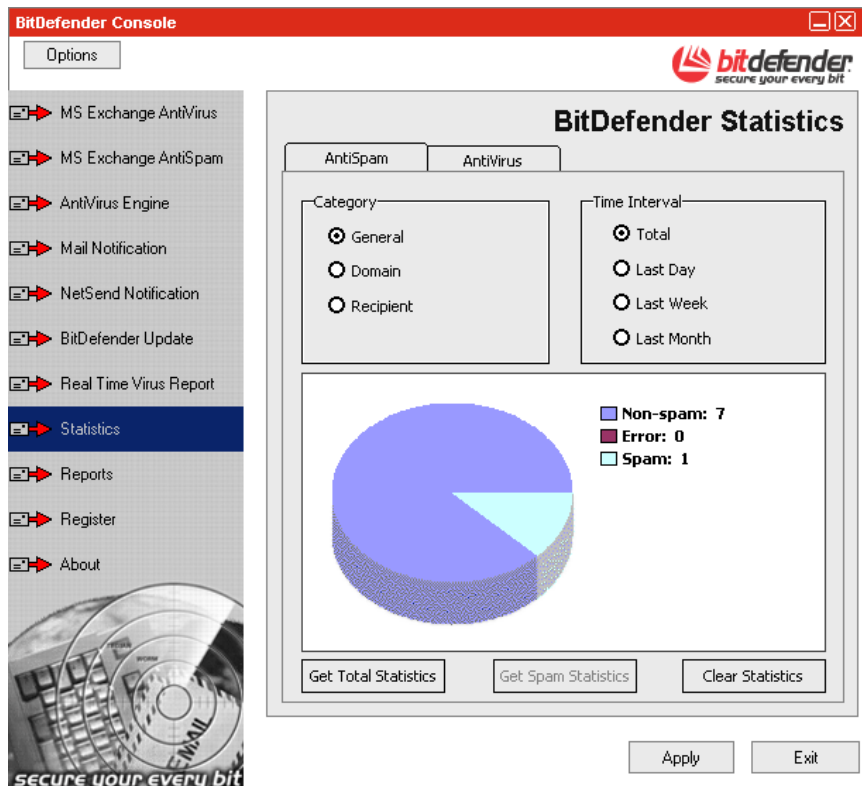


Figure 31

To create statistics, you must select:

- The category (**General**, **Domain** or **Recipient**);
- The time interval (**Total**, **Last Day**, **Last Week** or **Last Month**).

After selecting those you may click the **Get Total Statistics** button (to view the statistics regarding the mail activity) or click the **Get Spam Statistics** button (to view the statistics regarding the spam activity).

Reports

To see the reports regarding the antispam activity click **Reports** from the management console. The section opens default in the **AntiSpam** pane.

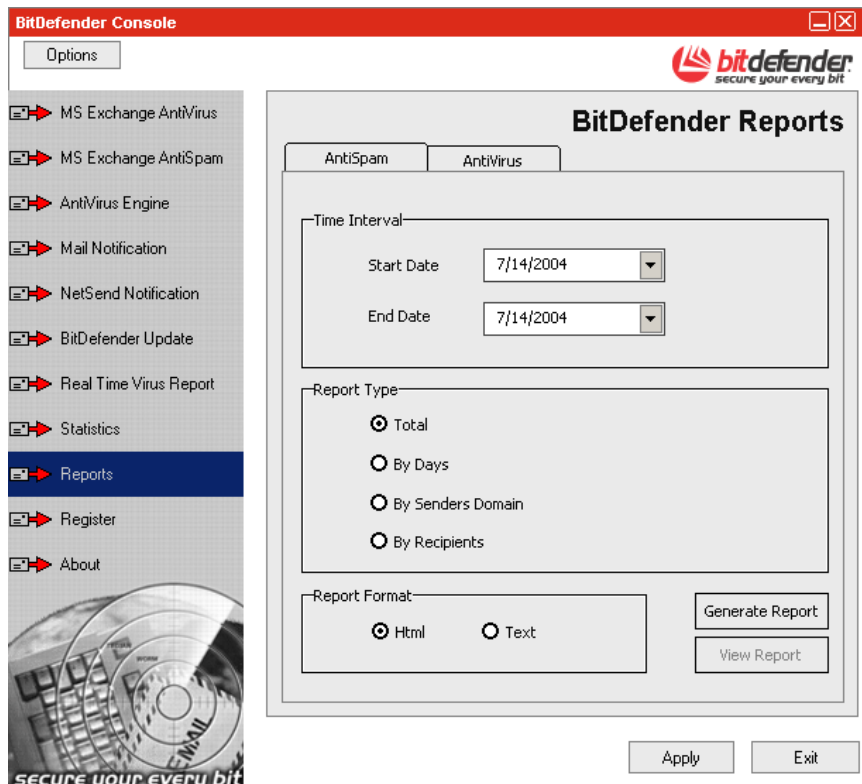


Figure 32

In this section you can generate a report file and you can see it.

Creating a report file

To create a report file, you must select:

- The time interval;
- The report type (**Total**, **By Days**, **By Senders Domain** or **By Recipients**);
- The report format (**Html** or **Text**).

After selecting those you may click **Generate Report**. The new reports are located in `program files\common files\softwin\reports`

Viewing a report file

The information contained in a report file can be viewed by clicking the **View Report** button. You can view: the number of the spam messages, the number of the non-spam messages and the number of errors (when BitDefender failed to analyze the message).

Product Update

BitDefender for MS Exchange 2003 was designed with a function for automatic update of the AntiVirus & AntiSpam engines. Every 8 hours the update function is launched. It connects to the BitDefender upgrade server and in case an update is found, it will be made transparently, without administrator's intervention, by downloading the files.

Updates come in three flavors:

- **Updates for AntiSpam engines** - new rules will be added to the heuristic & URL filters; this will help increase the effectiveness of your Antispam engine. This update type is also known as **AntiSpam Update**;
- **Updates for AntiVirus engines** - as new threats appear, the files containing virus signatures must be updated to ensure permanent up-to-date protection against them. This goes under the name of **Virus Signatures Update**;
- **Product upgrades** - when a new product version is released, new features and scan techniques are introduced to the effect of improving the product's performance. This update type is also known as **Product Update**.

In case you haven't already opened the management console, you can access it from the Windows Start menu, following the path **Start → Programs → BitDefender for MS Exchange 2003 → BitDefender for MS Exchange 2003**.

In the management console, click **BitDefender Update**.

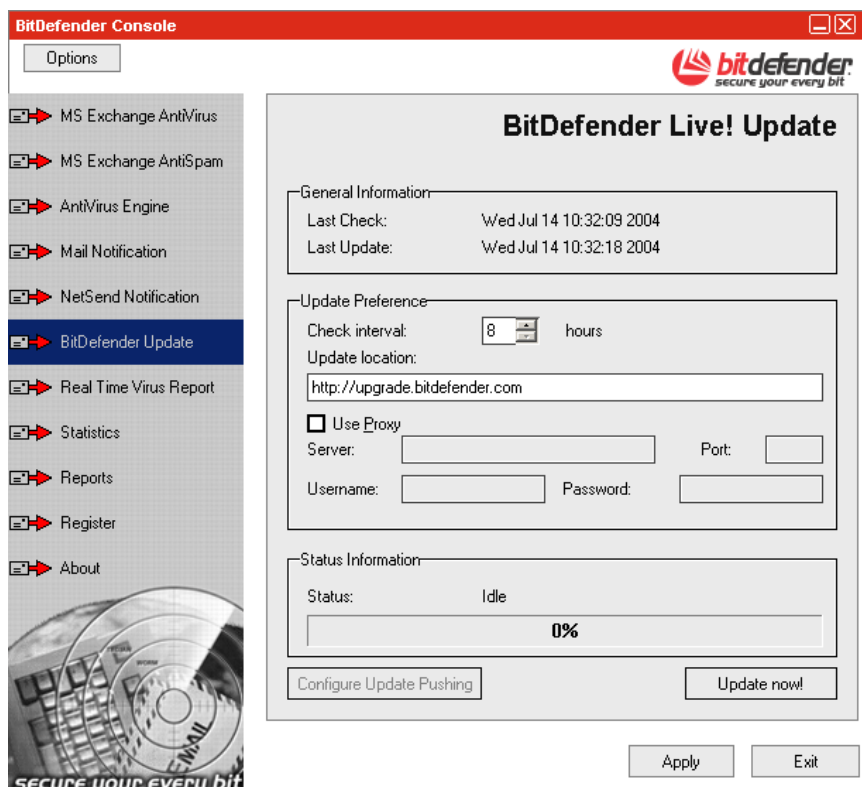


Figure 33

The section contains 3 subsections:

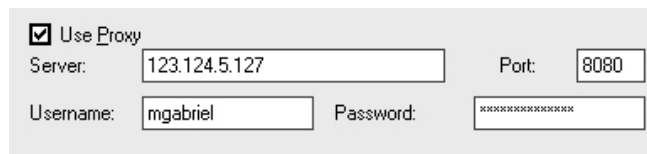
- **General information** contains the date and time of the last check and update.
- **Update preference** allows the selection of the update-checking interval. By default this is 8 hours. If you want to change it, type a new interval in the **Check interval** field. If you want to modify the update location, type in a new one in the field **Update location**, then click **Apply**.

In this subsection the options for the product update configuration can be found. These are necessary in case your network uses a proxy server with/without authentication. In this case, select the **Use proxy** check box.

The following options will be activated:

- ➔ **Server** - type in the IP of the proxy server.
- ➔ **Port** - type in the port the server uses to connect to the proxy server.
- ➔ **Username** - type in a user name recognized by the proxy.
- ➔ **Password** - type in the valid password for the previously specified user.

See the example below:



The screenshot shows a configuration form for proxy settings. At the top left, there is a checked checkbox labeled "Use Proxy". Below it, there are four input fields: "Server:" with the value "123.124.5.127", "Port:" with the value "8080", "Username:" with the value "mgabriel", and "Password:" with a masked password represented by asterisks.

Figure 34



It is possible that you need to also type the domain name in order to authenticate. You can introduce **domain\user** instead of the user name.

- **Status information** shows the status of the update process.

Click **Configure Update Pushing** to configure the update pushing feature. BitDefender will initiate an update upon receipt of a specially crafted "update announcement" message from BitDefender Labs (subscription service).

Click **Update now** if you wish to launch the update immediately. The application will contact the upgrade server and will update the engines if any update is found.

Click **Apply** in order to save the changes

Best practices

1. After the installation process is over, please [register](#) the product.
2. Select the action to be taken on infected messages. Enter the [AntiVirus Engine](#) section and select the desired action: disinfect, delete, move to Quarantine or ignore (no action). For disinfect you can select a second action in case the disinfection fails.
3. Select the action to be taken on spam messages. Enter the [MS Exchange AntiSpam](#) section and select the desired action: redirect, reject, delete or ignore (no action). For redirect and ignore you can configure BitDefender to modify the subject.
4. In the same window, select the **Add header** check box. The result is that the header of all the messages (spam or not) will be modified.

If you receive an e-mail that you think is spam, but BitDefender didn't tag it you can check the spam score in the e-mail properties.

5. Verify that BitDefender is working with the GTUBE & EICAR tests.

The GTUBE test consists in entering the `XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X` line in the body of an e-mail and send it to an user that has the e-mail on the server protected by BitDefender. BitDefender must tag as spam any message that contains this string.

The EICAR test consists in creating a file using a 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*`.

Save the file to any name with COM extension, for example EICAR.COM and send it as attachment to an user that has the e-mail on the server protected by BitDefender. BitDefender must treat this message as an infected one.



The string must be reproduced on a single line.

After sending those messages, access the **Statistics** section, where you can see if BitDefender is actually working.

6. Configure the AntiSpam filters: [Keyword filter](#), [White list](#), [Black list](#), [Charset filter](#), [URL filter](#) and [Heuristic filter](#).
7. If a virus is detected or an unexpected situation appears, there is the possibility of sending alarm messages by e-mail or by netsend.

Access the [Mail Notification](#) section or the [NetSend Notification](#) in order to configure BitDefender to send these notifications.



Examples of unexpected situations: license expiration, protection disabled, errors in client - server communication, errors while starting BitDefender and so on.

8. Configure the update. Enter the [BitDefender Update](#) section and if you are using a proxy check **Use Proxy** and type in the settings. You can change the update interval (the default interval is 8 hours).

Configure the update pushing feature. Click **Update now** in order to update the BitDefender AntiSpam & AntiVirus engines.

Frequently Asked Questions

- 1. Q:** What is spam?
A: Spam is unsolicited commercial e-mail.
- 2. Q:** I have blocked an e-mail address but I continue to receive e-mail messages from that address, why?
A: If you receive spam from an address you have blocked, please make sure that the address is not in the [White list](#), too. The [White list](#) has precedence over the [Black list](#).
- 3. Q:** I receive e-mail messages tagged as SPAM from an address contained in the [White list](#)?
A: A rule is created in the [Keyword filter](#) to tag that messages as SPAM.
- 4. Q:** How can I tell if BitDefender is actually working?
A: Use the GTUBE & EICAR tests described in [Best practices](#) section at step 5.
- 5. Q:** What is the [White list](#)?
A: Is a list of all the e-mail addresses from which you always want to receive messages, regardless of their content.
- 6. Q:** What is the [Black list](#)?
A: It is a list of all the e-mail addresses from which you don't want to receive messages, regardless of their content.
- 7. Q:** What is the [Charset filter](#)?
A: It is a filter that blocks all the e-mail messages written in Cyrillic and/or Asian.
- 8. Q:** What is the [URL filter](#)?
A: Is a filter that searches the messages for links and it will compare those found with the links from the [URL filter](#) BitDefender database. In case of a match +45 will be added to the spam score.
- 9. Q:** What is the [Heuristic filter](#)?
A: It is a filter that performs a set of tests on all the message components, (i.e. not only the header but also the message body in either HTML or text format), looking for words, phrases, links or other characteristics of spam. The result is that it will add a spam score to the e-mail.
- 10. Q:** Where does the spam go?
A: It depends on what action have you selected (in the [AntiSpam](#) section).
- 11. Q:** How can I set BitDefender to send mail notification in case a virus is found?
A: Access the [Mail Notification](#) section and follow the instructions as described in the help file.

- 12.Q:** How can I set BitDefender to deliver netsend notification in case a virus is found?
A: Access the [NetSend Notification](#) section and follow the instructions as described in the help file.
- 13.Q:** How do I uninstall BitDefender?
A: Follow the path: **Start** → **Programs** → **BitDefender** → **Repair or Uninstall** and in the window that will appear click the **Remove** button. This will start the uninstall process.
- 14.Q:** How can I update BitDefender?
A: By default, BitDefender will automatically update every 8 hours. But you can also update manually or change the time interval for the automatic update in the [BitDefender Update](#) section.
- 15.Q:** Why is it necessary to update the BitDefender AntiSpam engines?
A: Every time you perform an **AntiVirus Update** new virus definitions will be added to the antivirus scanning engines and when you perform an **AntiSpam Update** new rules will be added to the URL & Heuristic filters (this will help increase the effectiveness of your AntiSpam engine).
- 16.Q:** How can I disable BitDefender?
A: You have to disable:
- the AntiVirus engine - access the [MS Exchange AntiVirus](#) section and remove the mark in the check box corresponding to **Enable Exchange AntiVirus Integration**;
 - the AntiSpam engine - access the [MS Exchange AntiSpam](#) section and remove the mark in the check box corresponding to **AntiSpam Proxy is Enabled**.
- 17.Q:** Where do I enter my serial number (license key)?
A: You must access the [Register](#) section, select the product, type in the serial number, click **Change Registration** and click **Apply**.
- 18.Q:** What are the system requirements?
A: You can see the system requirements [Installation](#) section.

BitDefender Enterprise Manager Integration

BitDefender Enterprise Manager Description

BitDefender Enterprise Manager integrates BitDefender products into one watertight security solution. Version 2.2 takes network protection one step further with support for WMI administration tasks. It allows for full automation of routine tasks (including upgrades and updates), while letting the administrator install clients and execute tasks from anywhere in the network, in a safe and secure manner.

BitDefender introduces a new tool designed to facilitate administrative control over large networks. BitDefender WMI Scripts v1.1 (Server Add-On) implements tasks based on WMI (Windows® Management Instrumentation). These tasks can be executed across the BitDefender Enterprise Manager network. WMI server add-on is available with Enterprise v2.2.

BitDefender Enterprise Manager is created with the requirements of today's corporations in mind. It considerably reduces administration costs for complex networks. Excellent protection is achieved while keeping cost per ownership and administrator workload low.

The top solution for complex networks security

- New server add-on available: BitDefender WMI Scripts v1.1 (Server Add-On);
- Meet the security needs of large networks;
- Integrate your BitDefender products into one watertight security solution;
- Create BitDefender Enterprise Manager clients automatically and remotely;
- Manage the networked clients, protection tasks and reports;
- Run WMI tasks to remove software, and get hardware and system information;
- Receive real-time security alerts from networked clients;
- Generate and display detailed reports and statistics;
- Program the execution of recurring operations;
- Use the management console to configure the products installed on workstations;
- Create groups of BitDefender clients for easy administration;
- Set up an upgrade location within your local network;
- Stand by and watch as Live! Update upgrades your protection with the latest product versions and signature files or restores your BitDefender products;
- Enjoy 24/7 tech support in a variety of languages.

BitDefender Enterprise Manager Main Features

KEY FEATURES

BENEFITS

Easy, portable installation

The BitDefender Enterprise Manager Server and Console don't need to be installed on one and the same dedicated server machine. Any computers running Windows NT4.0/2000/XP will do. A wizard is available to guide you through the installation process. BitDefender Enterprise Manager allows centralized multi-platform integrated installation.

Remote management

The BitDefender Enterprise Management Console can be installed anywhere in the network. The Console can perform remote configuration of the server and remote management of the clients.

Fast, Free Live! Updates

Intelligent update of antivirus protection, without user intervention. Live Update can be performed from a local web server, over the Internet, directly or through a proxy server. The product is able to repair itself if necessary, by downloading the damaged or missing files from BitDefender servers. BitDefender license owners benefit from free virus definitions update and free upgrades.

Completely automated response to new virus outbreaks

BitDefender Enterprise Manager can be configured to automatically retrieve the newest virus definitions available on BitDefender servers, to deploy them throughout the network, to start scan processes at different preset network levels, to delete or repair suspicious or infected files and to generate detailed reports of all network events. These advantages enable IT Managers to rely on the most complete antivirus protection and on an unprecedented data security level.

Unlimited Scalable Solution

Management of huge networks, without affecting product stability or reliability in any way.

Detailed Reports and Statistics

BitDefender AntiSpam comes with a separate reports module, which provides daily, weekly or monthly statistics organized by categories. The reports can be generated and viewed in the administration console.

Intelligent Alerts

Intelligent alert features warn the system administrator through Console alerts and/or e-mail about events occurring in the network, such as: virus detection, failure to run security tasks, etc. In the control panel window, the admin can spot immediately which stations need their attention.

Secure Communication

Communications between the various product modules, clients and server add-ons is achieved through secure channels.

24/7 professional technical support

Qualified support representatives and an online database are available to our customers at no extra cost.

Supported clients

BitDefender Enterprise Manager v2.2 smoothly integrates with and manages:

Workstation clients

- BitDefender Standard Edition v7.1 + (Server Add-On)
- BitDefender Professional Edition v7.1 + (Server Add-On)
- BitDefender WMI Scripts v1.1 (Server Add-On)

Server products

- BitDefender for Mail Servers (Win SMTP) v1.6 +
- BitDefender for File Server v1.6 +
- BitDefender v1.6+ for MS ISA
- BitDefender v1.6+ for Exchange 5.5
- BitDefender v1.6+ for Exchange 2000
- BitDefender for MS Exchange 2003
- BitDefender AntiSpam for Mail Servers (Win SMTP Proxy)

System requirements

- Microsoft Windows Network (TCP/IP)

For BitDefender Server:

- Intel Pentium compatible processor
- Minimum free disk space: 100MB
- RAM: 64MB
- Operating systems: Windows NT SP6, Windows 2000 or Windows XP

For BitDefender Management Console:

- Intel Pentium compatible processor
- RAM: 64MB
- Minimum free disk space: 10MB
- Operating system: Windows 98 SE/NT SP6/Me/2000/XP Internet Explorer 4.0 or superior

For BitDefender Local Manager:

- Intel Pentium compatible processor
- RAM: 32MB
- Minimum free disk space: 10MB
- Operating system: minimum Windows 98 SE

For BitDefender Deployment Tool:

- Operating system: Windows NT SP6/ 2000/XP

For BitDefender Update Server:

- Intel Pentium compatible processor
- Minimum free disk space: 100MB (for updates)
- Minimum 64MB RAM
- Operating systems: Windows NT4.0 SP6, Windows 2000 or Windows XP Internet Explorer 5.0 or higher

How does BitDefender Enterprise Manager work?

BitDefender Enterprise Manager is a scalable, superior solution for centralized management of antivirus protection in complex networks. BitDefender Enterprise Manager combines both the advantages of defining and controlling network security policies, and advanced technologies of data filtering in order to cover any major security breach.

Real time reporting of network attacks, and the ability to evaluate them in a centralized manner allow for a fast, efficient response. **BitDefender Enterprise Manager** considerably reduces administration costs for complex networks, ensuring the most efficient protection of vital company information.

BitDefender Enterprise Manager 2 is divided into five parts:

BitDefender Server

It is the most important of the **BitDefender Enterprise Manager** components; its purpose is to manage the information received from the workstations, assign and maintain different security tasks such as:

- install /uninstall of the anti-virus product;
- anti-virus scanning;
- scheduled scanning;
- virus definitions database update;
- remote changing of security options of BitDefender products installed on workstations;
- detailed reports and statistics generation
- configuring of all the BitDefender products installed.

The tasks received from the user through the management console are forwarded to the workstations in order to be executed, while the information received from the workstations is processed and organized into reports. The reports are sent to the management console where they can be viewed and interpreted by the administrator.

The server can be dynamically extended to perform various other security-related tasks that the customers may need. The server can be password protected. The password can be set in the management console.

BitDefender Local Manager

This component is installed on each workstation, which the administrator may want to administrate through **BitDefender Enterprise Manager**. Through this component, BitDefender Server communicates with the workstations from the network and assigns different tasks to the BitDefender products installed on them. However, the remote deployment of other BitDefender products is possible only after the deployment of **BitDefender Local Manager**. This component maintains a local database with information concerning each BitDefender product installed on that workstation.

BitDefender Enterprise Management Console

This component represents the graphic user interface (GUI), especially created to allow the communication between the user and **BitDefender Server**. From the user's point of view, the management console performs the following tasks:

- Ensures easy administration of the workstations, by organizing them into workgroups;
- Remotely installs the BitDefender products;
- Assigns new tasks to the BitDefender products installed on the workstations;
- Sets the tasks so that they may be executed on one workstation only, on groups' or on all the workstations from the network;
- Performs common operations like: scheduled scanning, virus definitions updating and protection option configuration;
- Displays alerts that are generated when tasks fail (in order to find the source of these errors) or when suspect / infected files are found on the workstations
- Can create and display different reports and statistics.

Note

You may install several management consoles in a certain network. However it is strongly advised that only one management console should be connected to the BitDefender server at a certain moment. Otherwise, multiple connections to the same server may compromise the functionality of the management console.

BitDefender Deployment Tool

This is a component independent of all the others. It performs remote deployment of the **BitDefender Local Manager**, eliminating the necessity to locally install it on each workstation. However, on some operating systems (Microsoft Windows 9x) this local deployment is a necessity. In case the remote deployment fails, you can send the **BitDefender Local Manager** via e-mail or copy it from a shared folder and install it by executing the e-mail attachment.

BitDefender Update Server

This component allows you to set up an upgrade location within your local network. This way you needn't worry about updating the products installed on computers that are not connected to the Internet, achieving, at the same time, faster updates and reduced Internet traffic.

Note

You must share the folder where you downloaded the updates in order to make them available for the network clients.

The **BitDefender Update Server** is easy to configure through an intuitive step-by-step wizard. It will help you get the latest updates for all BitDefender products.



The only visible components to user are BitDefender Enterprise Management Console and BitDefender Deployment Tool.

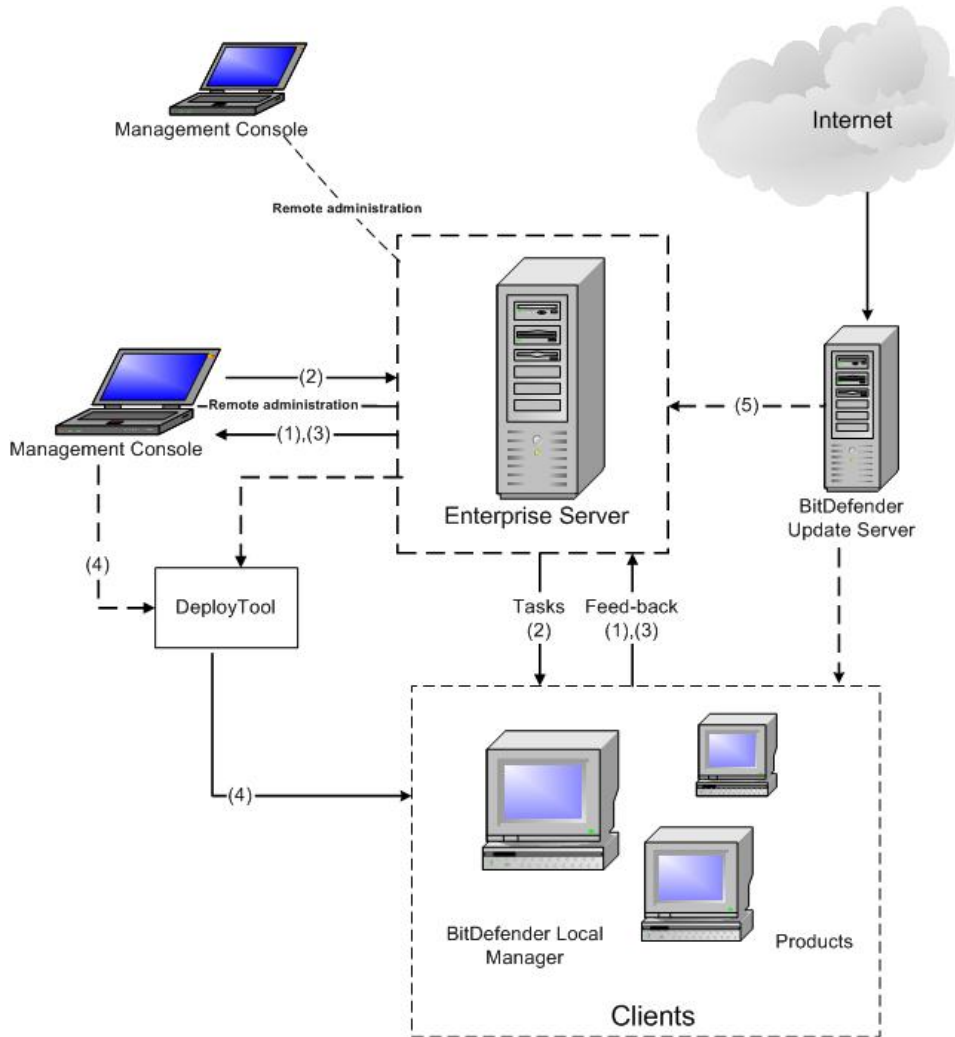


Figure 35

In the above picture there are presented the architecture and the way the product works in a simplified manner.

Five information flows can be identified and they can be described as follows:

1. **BitDefender Deployment Tool** sends the task to install **BitDefender Local Manager** to the workstations.
2. **BitDefender Local Manager** creates a database with all the BitDefender products already installed on the workstations and then sends the information to the **BitDefender Server**. The Server takes it over and sends it to **BitDefender Enterprise Management Console**, where the administrator can access it.
3. The user selects the protection options for all BitDefender products, through the management console. These options are received by **BitDefender Server** and forwarded to the **BitDefender Local Manager** corresponding to each workstation. Further on, BitDefender products will execute the commands selected by the user through the management console.
4. The results of the commands' execution on the workstations are sent to **BitDefender Server**. Depending on the user's option, this information is used for creating reports that can be viewed through the management console.
5. **BitDefender Update Server** sets up an upgrade location within your local network, in a folder that must be shared in order to make the updates available to the network clients. Using the **Management Console** the administrator can create update tasks from this location. The users from the client workstations can also choose to update their antivirus product from this location.


Additional Task Templates

BitDefender for MS Exchange 2000 deeply integrates with **BitDefender Enterprise Manager**, meaning you can configure this product from the Enterprise Management Console.

 **Note**

The **BitDefender for MS Exchange 2000** must be installed on a **BitDefender Enterprise** client. This means **BitDefender Local Manager** is already installed on that workstation or it will be installed in order to import the newly created tasks from that workstation.


After the **BitDefender for MS Exchange 2000** installation process is over, access the **Clients** section (from the **BitDefender Enterprise Manager**) in one of the following ways:

- Click **Clients** from the configuration bar;
- On the **Clients&Groups** menu, click **Go to Clients Pane**;
- Click the **Open Clients Pane**  button from the toolbar;
- Use the shortcut **CTRL+1**.

The next step is to import tasks templates from the workstation that has installed **BitDefender for MS Exchange 2000**. You can proceed in one of the following ways:

- Select the client and from the **Clients&Groups** menu, point **Clients**, click **Import Tasks Templates from Selected Clients**;
- Right-click the selected client and from the shortcut menu click **Import Tasks Templates from Selected Clients**.

The imported tasks templates will become visible in the **Tasks Templates** section. To access it you should do one of the following:

- simply click **Task Templates** from the top side of the Tasks window;
- click **Tasks** from the main menu and then choose **Go to Task Templates** pane;
- use the shortcut **CTRL+3**;
- click the **Go To Task Templates Pane**  button from the toolbar.

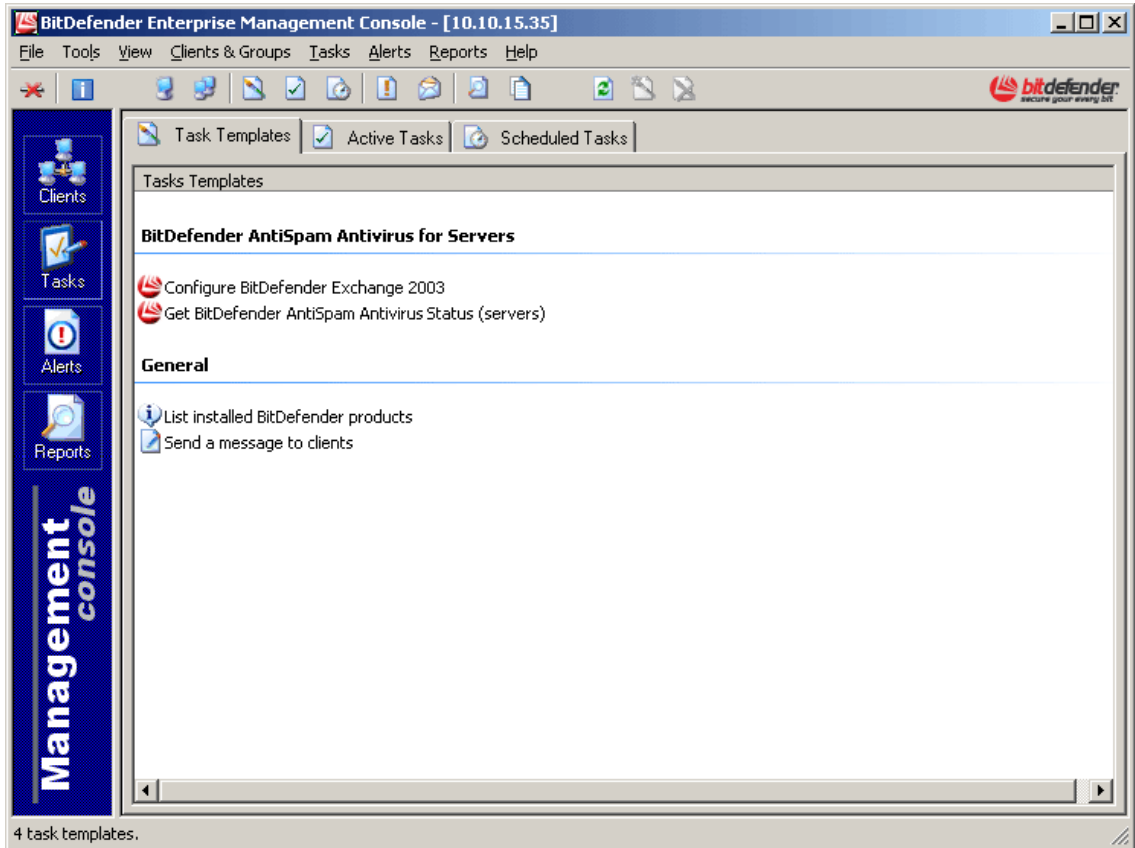






Figure 36

This section contains templates files necessary for different tasks. By double-clicking any of these icons, you will launch the wizard that will help you selecting the protection options. You can view the following task templates:

BitDefender AntiSpam & AntiVirus for Servers

-  [Configure BitDefender Exchange 2003](#) – to configure **BitDefender for MS Exchange 2003**;
-  [Get BitDefender AntiSpam AntiVirus Status \(server\)](#) - to receive information about the antivirus status.

General

-  [List installed BitDefender products](#) - to show a list with all the BitDefender products installed on the selected workstations;
-  [Send a message to clients](#) - to send a message to specified clients.

Configuring BitDefender for MS Exchange 2003


In order to configure the product on one or more workstations, you must double-click the  **Configure BitDefender Exchange 2003** icon (from the **Task Templates** pane). This will launch the wizard, which will guide you through the configuration process:



Figure 37

Configuration steps:

1. Click **Next** in order to continue or click **Cancel** if you want to quit configuration.
2. Here you can configure the **BitDefender for MS Exchange 2003**. The configuration options are grouped in six categories: **Exchange 2003**, **BitDefender AntiVirus Engine**, **BitDefender AntiSpam Engine**, **BitDefender Update**, **Mail Notification**, **NetSend Notification** and **Real Time Virus Report**.

Note

One can observe that some options, although the "+" sign appears, cannot be opened. The reason is that these options weren't selected yet. You will observe that if you select them, they can be opened.

Exchange 2003

Select the checkbox corresponding to **Is active** in order to enable the BitDefender Antivirus engine.

Background Scanning

Means scanning of all folders with a low priority. When an object, that has been checked by background scanning, is requested it will not be scanned again (unless a virus definition update has been made).

The information store will use one thread, per database, running at low priority to perform background scanning of the messages and attachments. Once the background scanning is completed, the thread is terminated. These threads are not part of the global virus-scanning thread pool used for on-access scanning.

Select this option in order to optimize the scanning process.

Proactive Scanning

When a message is submitted to the information store, either via a client or a transport agent, it is placed in the global scanning queue with a low priority. If and when there are threads available in the thread pool and no high priority item remains to be scanned, each item with the low priority is submitted for scanning.

If an item is in the low priority list and a client attempts to access the message, the item will be reprioritized and marked with high priority. It will also be removed from the low priority list. If this setting is disabled, and messages were not submitted for scanning for any reason, they will be scanned when they are accessed

Transport Scanning

Messages may be scanned at the transport level using this option. This prevents infected messages from entering the Exchange organization.

Messages are submitted to the Exchange store from the transport engine, allowing access to messages via the VSAPI. Following scanning, messages are resubmitted to transport for delivery to their destination. Any message scanned at the gateway will be rescanned on the back-end server. The transport scanning functionality is not activated by default.

Scanning Plain Text

Select this option in order to scan body messages in plain text format.

Scanning RTF

Select this option in order to scan body messages in RTF (Rich Text Format) format.

Scanning Timeout

You may introduce here the maximum time allocated for scanning an object. If the scanning process is not completed before the time out, an error is returned and the access to the un-scanned object is prohibited.

BitDefender AntiVirus Engine

Selecting the action on infected messages

BitDefender allows selecting two actions in case an infected message is found. The second action is enabled only in case the first action you selected is to disinfect the infected messages.

You can select one of the following actions:

First Action	Description
Ignore	The infections found are ignored and the messages will be delivered to the mail recipients, along with the infected part*, without any reaction.
Disinfect	The infected part* of the message will be disinfected. If the disinfection fails, a second action will be taken.
Delete	The infected part* of the message will be deleted. A <code>virus info.txt</code> will be delivered to the mail recipient informing him about the infection and the action BitDefender took.
Move to quarantine	The infected file will be isolated in the quarantine zone.

Second Action	Description
Ignore	In case the disinfection of the message fails, this is delivered to the mail recipient without any change and still containing the infection.
Delete	If the disinfection fails, the infected part* will be deleted. A <code>virus info.txt</code> will be delivered to the mail recipient informing him about the infection and the action BitDefender took.
Move to quarantine	If the disinfection fails, the infected part* will be moved to the quarantine folder. A <code>virus info.txt</code> will be delivered to the mail recipient informing him about the infection and the action BitDefender took.

* the body or the attachment(s) of the messages

TIP: We recommend using 1st action: **Disinfect**, 2nd action: **Delete**.

Setting the Quarantine zone

The default location of the quarantine zone is: `C:\Program Files\Common Files\Softwin\ADD-ONS\quar`. If you want to change it, type in the complete path in the **Quarantine location** field.

BitDefender AntiSpam Engine




Select the checkbox corresponding to **BitDefender AntiSpam Engine** in order to be protected against spam.

Setting the Spam Threshold

The default **Spam Threshold** is 90. If you reduce this value the filter will let some spam through. If you increase this value very little spam will pass, but some legitimate messages may be tagged as spam.

Selecting the action on spam messages

You must select one of the following actions:

Action	Description
Redirect	<p>The result is that the spam messages are redirected to a specified e-mail address. Select Redirect mail check box and type the address where spam will be delivered in the Mail to redirect field. You can type a local e-mail address or one from another SMTP server.</p> <p> You must specify only one address. If the Mail to redirect field is empty or the e-mail address is invalid the spam messages will not be redirected.</p>
Reject	<p>The result is that the spam messages are rejected with a 550 SMTP error code.</p> <p> Action not recommended.</p>
Delete	<p>The result is that the spam messages are deleted.</p> <p> Action not recommended.</p>
No Action	<p>The result is that the spam messages will be delivered to the e-mail recipients without any reaction.</p>
Add Header	<p>The result is that the header of all the messages (spam or not) will be modified. Select the Add Header check box and type the desired header in the Header Name field.</p> <p>The default case is <code>X-BitDefender-Spam</code> as header, <code>Yes(\$score)</code> as spam value and <code>No(\$score)</code> as non-spam value. When a spam is detected the header will be <code>X-BitDefender-Spam: Yes(x%)</code> (where <code>x</code> - represents the spam score). All non-spam messages will have as header <code>X-BitDefender-Spam: No(x%)</code> (where <code>x</code> - represents the spam score).</p>
Modify Subject if Spam	<p>The result is that the subject of the spam messages will be modified. Select Modify Subject if Spam check box and introduce the desired subject in the Subject Pattern field.</p> <p>The subject must be specified like:</p> <ul style="list-style-type: none"> • <code>[SPAM]</code> - all e-mail messages considered spam will have the subject <code>[SPAM]</code>; • <code>[SPAM]\$subject</code> - all e-mail messages considered spam will have the subject <code>SPAM</code> followed by the original subject - this is default; • <code>[\$score% SPAM]\$subject</code> - all e-mail messages considered spam will have the subject <code>[x% SPAM]</code> followed by the original subject (where <code>x</code> - represents the spam score). <p>For example we have a spam message with the original subject line <code>Very important!</code>. The subject line will be changed to <code>[SPAM]</code> for the first case, <code>[SPAM] Very important!</code> for the second case and <code>[x% SPAM] Very important!</code> for the third case (where <code>x</code> - represents the spam score).</p>

Used filters

You can select or deselect one (or more) of the following filters: the **Keyword Filter**, the **White/Black Lists**, the **Heuristic filter** and the **URL filter**. Select the filters you want to be activated for this task.

The **Heuristic filter** contains the **Reject charsets** option. With this option you can block all the e-mail messages written in Cyrillic and / or Asian charsets. Click **Reject charsets** and select **Asian** and / or **Cyrillic** check box(es).

Advanced options

Connections that are authenticated are trusted, therefore they should be allowed to bypass spam detection. The **BitDefender AntiSpam Engine** should only be activated for messages that have been submitted anonymously or are not on a safe connection list. If you select the checkbox corresponding to **Check authenticated connection** all the messages will be scanned by the **BitDefender AntiSpam Engine**.

BitDefender Update

Every 8 hours the update function is launched. It connects to the BitDefender upgrade server and in case an update is found, it will be made transparently, without administrator's intervention, by downloading the files.

Select **BitDefender Update** to enter the update configuration settings.

- BitDefender allows the selection of the update-checking interval. By default this is 8 hours. If you want to change it, type in a new interval in the **Check interval** field.
- If you want to modify the update location, type in a new one in the field Main upgrade location. By default this is: <http://upgrade.bitdefender.com>.
- In case the company uses a proxy server check the option **Use proxy**. The following options will be activated:
 - ➔ **Proxy server** - type in the IP of the proxy server;
 - ➔ **Proxy port** - type in the port the server uses to connect to the proxy server;
 - ➔ **Proxy username, if needed** - type in a user name recognized by the proxy;
 - ➔ **Proxy password, if needed** - type in the valid password for the previously specified user.

Mail Notification

Click the **Mail Notifications** option and select the checkbox corresponding to **Enable** to activate this service. In order to send alerts via e-mail you must first specify some information in the section **Exchange Settings**:

- ➔ **Exchange mailbox** - type in the name of the mailbox you use to send alerts;
- ➔ **User name** - type in the user name;

Tip: The user must have rights on the specified mailbox.

- ➔ **Password** - type in the administration password.



It is necessary to type in a valid e-mail address for the Mail server; otherwise the server may decline to send an e-mail whose sender (e-mail address) is unknown to it.

- **Notify on Virus** - type in the person's e-mail address you want to be notified in case a virus is found;
- **Notify on Warning** - type in the person's e-mail address you want to be notified in case a special situation, such as disabling the BitDefender protection, appears;
- **Notify on Error** - type in the person's e-mail address you want to be notified when a disfunctionality of BitDefender appears. Such situations may occur, for example, because of the accidental deletion of some files or failure to load the AntiSpam engines;
- **Notify Sender** - select this option if you want to notify the sender if a virus is found in one of his e-mail messages;
- **Notify Receivers** - select this option if you want to notify the receivers if a virus is found in an e-mail addressed to them.

Note

If you want to send messages to more than just one mail recipient, these addresses must be separated by ",".

Netsend Notification

Click the **NetSend Notifications** option and select the checkbox corresponding to **Enable** to activate this service.

- **Notify on Virus** - type in the workstation you want to be notified in case a virus is detected;
- **Notify on Warning** - type in the workstation you want to be notified in case a special situation, such as disabling the BitDefender protection, appears;
- **Notify on Error** - type in the workstation you want to be notified when a disfunctionality of BitDefender appears. Such situations may occur, for example, because of the accidental deletion of some files or failure to load the AntiSpam engines.

Note

If you want to netsend alarms to more than one workstation, you can specify the names of the workstations separated by ";".

Real Time Virus Report

Click the **Real Time Virus Report** option and select the checkbox corresponding to **Enable** to activate this option. From the scroll down list, select the country where you live.

Check the option **Save settings as default** to keep the same configuration for the future tasks. Click **Next**.

3. You must select the clients and/or the groups.

If a group contains at least one client then a double click on that group's name or its corresponding icon will expand that group. You can choose to run the task on one or several clients. To select all the clients from a group select the check box left to the group's name.

Once you have selected the target workstations, click **Next**.

4. You can opt for an immediate or a programmed configuration. For an immediate configuration, select **Immediately** and specify the following:

- **Enter the task name** - type in a name for the task;
- **Enter the task description** - type in a short description of the task.

Once you specified all the information, click **Next** to view a summary description of the task.

For a scheduled configuration, select **Scheduled for later** and specify the following:

- **Enter the task name** - type in a name for the task;
- **Enter the task description** - type in a short description of the task;
- **Run the task** - it is a list with time intervals when the configuration process should run. You can select **One time only** - to configure at a specified moment;
- **Start date** - click the arrow corresponding to the field and select a day from the calendar that appears;
- **Start time** - type the hour when the configuration process will launch. You can use the corresponding arrows up/down.


Click **Next**.

5. The last window of the wizard contains all the information regarding the task.

Click **Finish**.

Depending on the task type, the task will appear in the **Active tasks** page, in case it is an immediate task or in the **Scheduled tasks** page, if it is a scheduled task.

Retrieving BitDefender status

In order to obtain the BitDefender status on one or more workstations, you must double-click the  **Get BitDefender AntiSpam AntiVirus Status (server)** icon (from the **Task Templates** pane). This will launch the wizard, which will guide you through the process:

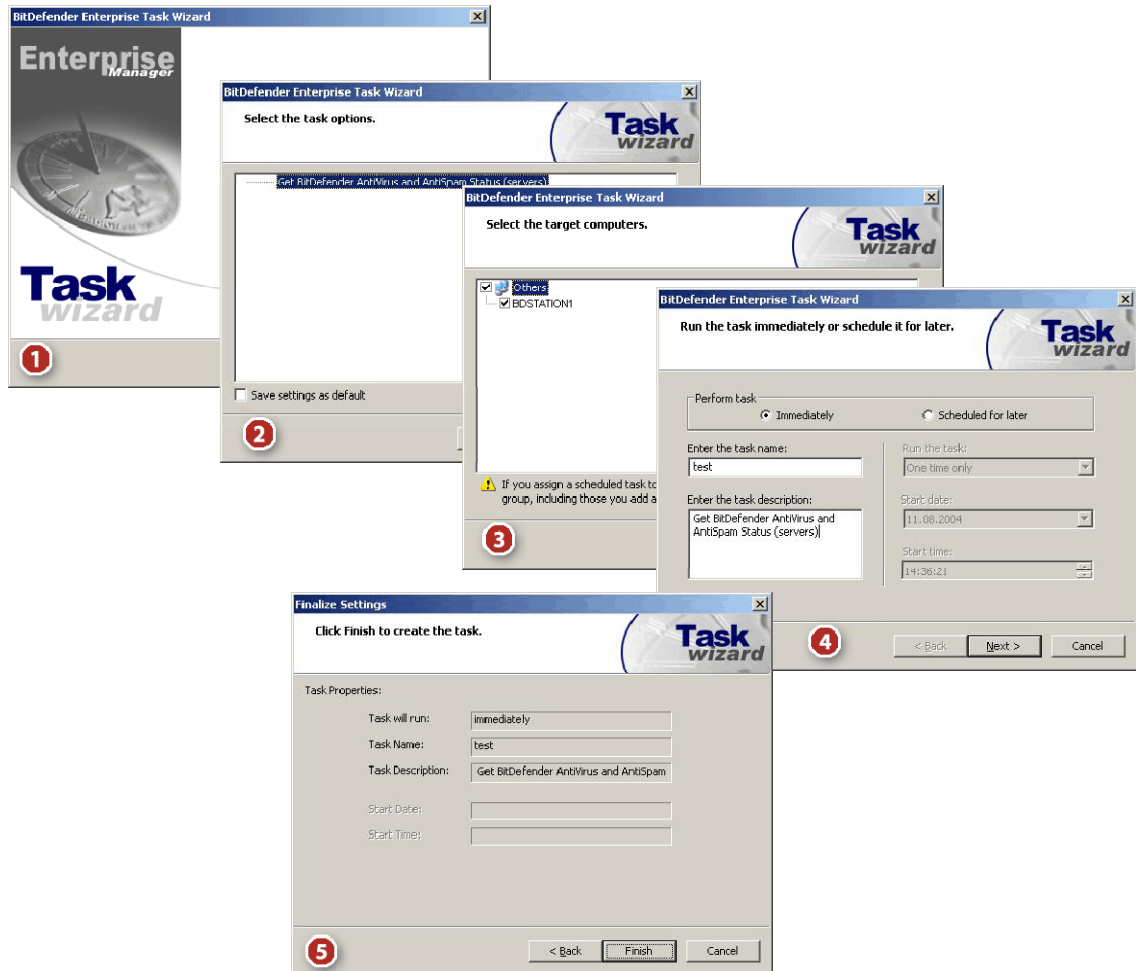


Figure 38

Task steps:

1. Click **Next** in order to continue or click **Cancel** if you want to quit.
2. Click **Next**.
3. You must select the clients and/or the groups.

If a group contains at least one client then a double click on that group's name or its corresponding icon will expand that group. You can choose to run the task on one or several clients. To select all the clients from a group select the check box left to the group's name.

Once you have selected the target workstations, click **Next**.

4. You can opt for an immediate or a programmed task. For an immediate task, select **Immediately** and specify the following:
 - ➔ **Enter the task name** - type in a name for the task;
 - ➔ **Enter the task description** - type in a short description of the task.

Once you specified all the information, click **Next** to view a summary description of the task.

For a scheduled task, select **Scheduled for later** and specify the following:

- ➔ **Enter the task name** - type in a name for the task;
- ➔ **Enter the task description** - type in a short description of the task;
- ➔ **Run the task** - it is a list with time intervals when the configuration process should run:
 - **One time only** - to run the task only once at a specified moment;
 - **Every hour** - to run the task every hour;
 - **Every 6 hours** - to run the task at every 6 hours;
 - **Every 12 hours** - to run the task at every 12 hours;
 - **Every day** - to run the task daily;
 - **Every two days (48 hours)** - to run the task at every 2 days;
 - **Every three days (72 hours)** - to run the task at every 3 days;
 - **Weekly** - to run the task weekly;
 - **Monthly** - to run the task monthly.
- ➔ **Start date** - click the arrow corresponding to the field and select a day from the calendar that appears;
- ➔ **Start time** - type the hour when the task will launch. You can use the corresponding arrows up/down.


Click **Next**.

5. The last window of the wizard contains all the information regarding the task.

Click **Finish**.

Depending on the task type, the task will appear in the **Active tasks** page, in case it is an immediate task or in the **Scheduled tasks** page, if it is a scheduled task.

Retrieving a list with all BitDefender products installed

In order to obtain a list with all BitDefender products installed on one or more workstations, you must double-click the  **List installed BitDefender products** icon (from the **Task Templates pane**). This will launch the wizard, which will guide you through the process:

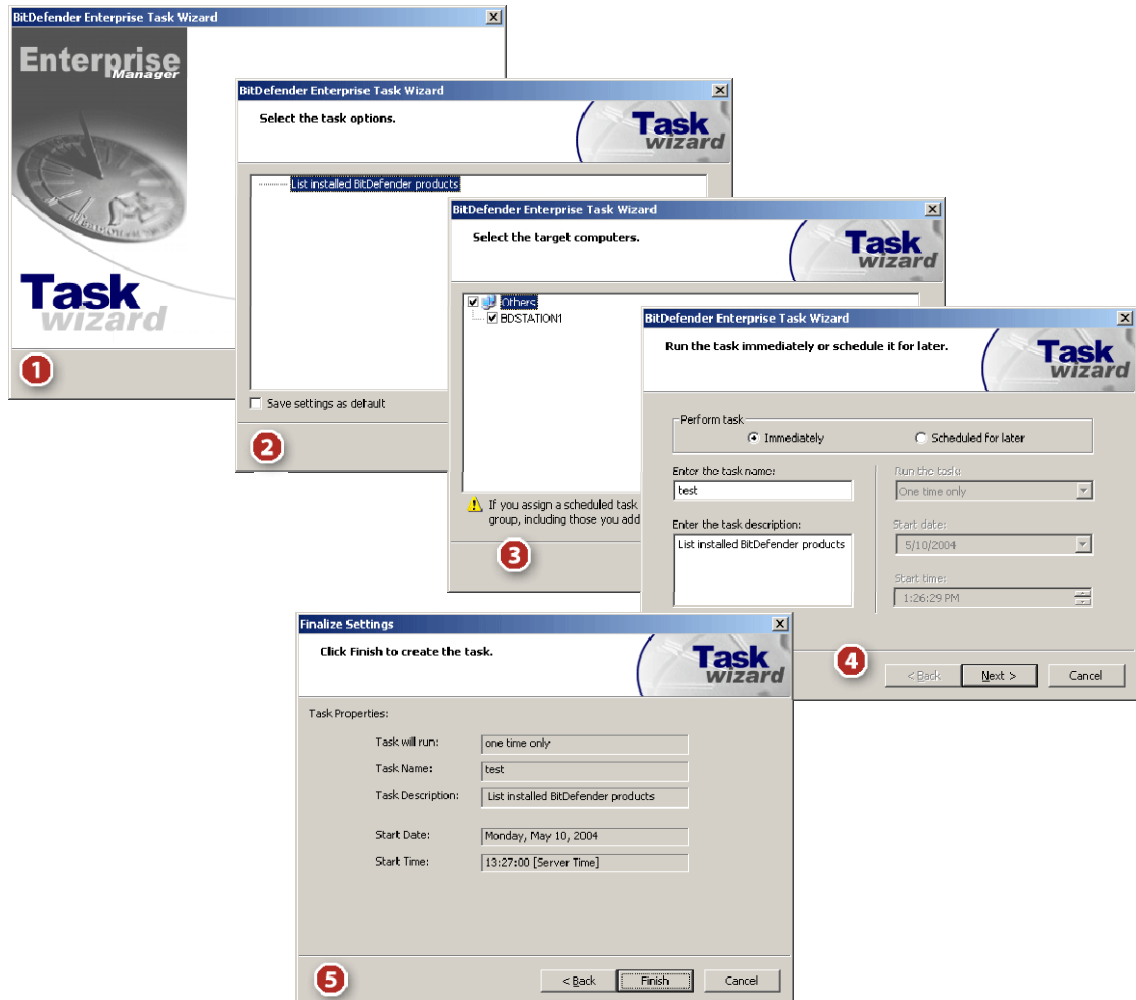


Figure 39

Task steps:

1. Click **Next** in order to continue or click **Cancel** if you want to quit.
2. Click **Next**.
3. You must select the clients and/or the groups.

If a group contains at least one client then a double click on that group's name or its corresponding icon will expand that group. You can choose to run the task on one or several clients. To select all the clients from a group select the check box left to the group's name.

Once you have selected the target workstations, click **Next**.

4. You can opt for an immediate or a programmed task. For an immediate task, select **Immediately** and specify the following:

- **Enter the task name** - type in a name for the task;
- **Enter the task description** - type in a short description of the task.

Once you specified all the information, click **Next** to view a summary description of the task.

For a scheduled task, select **Scheduled for later** and specify the following:

- **Enter the task name** - type in a name for the task;
- **Enter the task description** - type in a short description of the task;
- **Run the task** - it is a list with time intervals when the configuration process should run:
 - **One time only** - to run the task only once at a specified moment;
 - **Every hour** - to run the task every hour;
 - **Every 6 hours** - to run the task at every 6 hours;
 - **Every 12 hours** - to run the task at every 12 hours;
 - **Every day** - to run the task daily;
 - **Every two days (48 hours)** - to run the task at every 2 days;
 - **Every three days (72 hours)** - to run the task at every 3 days;
 - **Weekly** - to run the task weekly;
 - **Monthly** - to run the task monthly.
- **Start date** - click the arrow corresponding to the field and select a day from the calendar that appears;
- **Start time** - type the hour when the task will launch. You can use the corresponding arrows up/down.


Click **Next**.

5. The last window of the wizard contains all the information regarding the task.

Click **Finish**.

Depending on the task type, the task will appear in the **Active tasks page**, in case it is an immediate task or in the **Scheduled tasks page**, if it is a scheduled task.

Sending a message to clients

In order to send a message to one or more workstations, you must double-click the  **Send a message to clients** icon (from the **Task Templates** pane). This will launch the wizard, which will guide you through the process:

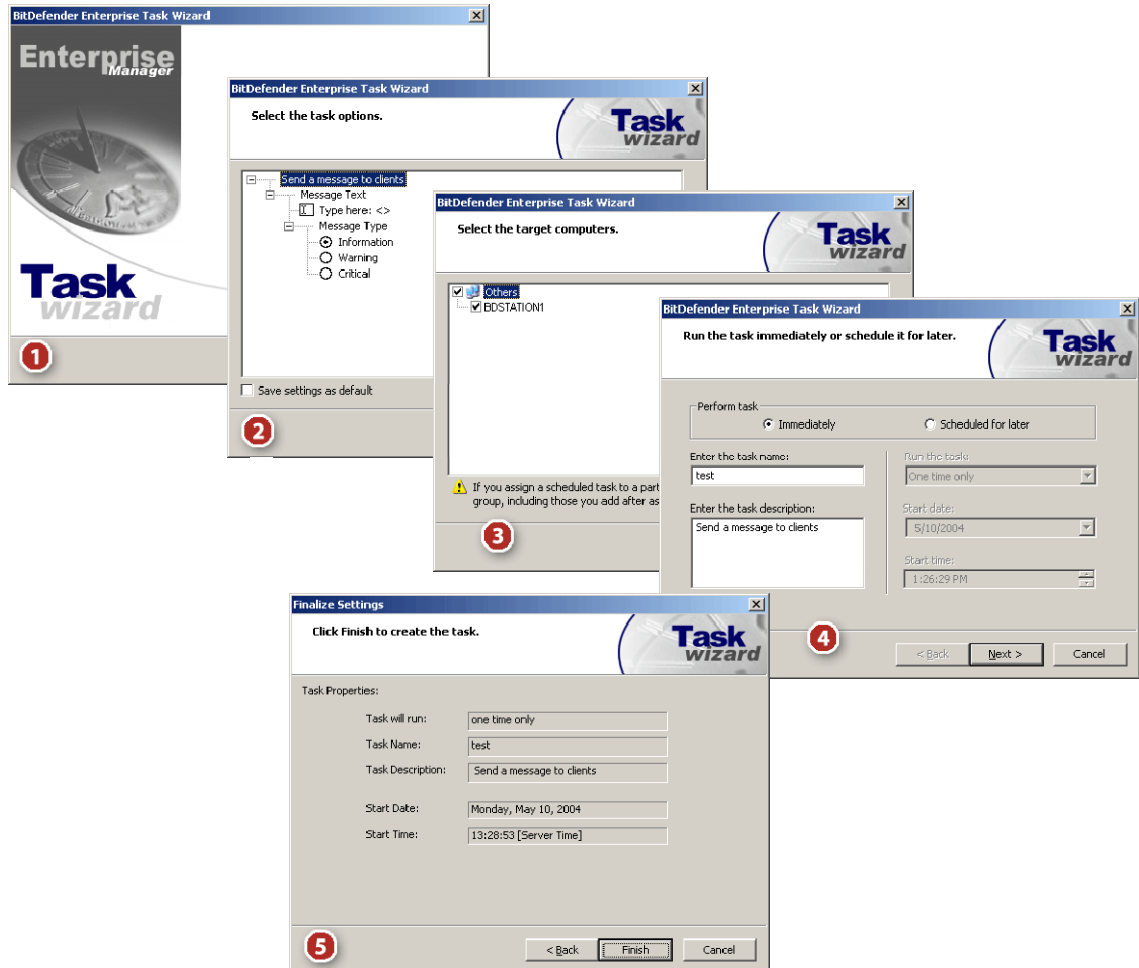


Figure 40

Task steps:

1. Click **Next** in order to continue or click **Cancel** if you want to quit.
2. Click the **Type here** field and introduce the message you want to send.

You can choose the significance level of each message by selecting the type of icon you want to associate with it (**Information**, **Warning** or **Critical**) from the **Message Type** section. Click **Next**.

3. You must select the clients and/or the groups.

If a group contains at least one client then a double click on that group's name or its corresponding icon will expand that group. You can choose to run the task on one or several clients. To select all the clients from a group select the check box left to the group's name. Once you have selected the target workstations, click **Next**.

4. You can opt for an immediate or a programmed task. For an immediate task, select **Immediately** and specify the following:

➔ **Enter the task name** - type in a name for the task;

→ **Enter the task description** - type in a short description of the task.

Once you specified all the information, click **Next** to view a summary description of the task.

For a scheduled task, select **Scheduled for later** and specify the following:

→ **Enter the task name** - type in a name for the task;

→ **Enter the task description** - type in a short description of the task;

→ **Run the task** - it is a list with time intervals when the configuration process should run:

- **One time only** - to run the task only once at a specified moment;
- **Every hour** - to run the task every hour;
- **Every 6 hours** - to run the task at every 6 hours;
- **Every 12 hours** - to run the task at every 12 hours;
- **Every day** - to run the task daily;
- **Every two days (48 hours)** - to run the task at every 2 days;
- **Every three days (72 hours)** - to run the task at every 3 days;
- **Weekly** - to run the task weekly;
- **Monthly** - to run the task monthly.

→ **Start date** - click the arrow corresponding to the field and select a day from the calendar that appears;

→ **Start time** - type the hour when the task will launch. You can use the corresponding arrows up/down.

Click **Next**.

5. The last window of the wizard contains all the information regarding the task.

Click **Finish**.

Depending on the task type, the task will appear in the **Active tasks page**, in case it is an immediate task or in the **Scheduled tasks page**, if it is a scheduled task.

Contact information

As a valued provider, BitDefender strives to provide its customers with an unparalleled level of fast and accurate support. The Support Center (which you can contact at the address provided below) continually keeps up with the latest threats. This is where all of your questions are answered in a timely manner.

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

Efficient communication is the key to a successful business. During the past 10 years SOFTWIN 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.

Sales department: sales@bitdefender.com

<http://buy.bitdefender.com>

Technical support: support@bitdefender.com

Phone: 0040-21-233 07 80

Product web site: www.bitdefender.com

Find a local distributor: www.bitdefender.com/partner_list/

Address:

SOFTWIN
5th Fabrica de Glucoza St.
PO BOX 52-93
Bucharest, ROMANIA