bitdefender

Security for MS Exchange

User's guide

Antivirus

Antispam

Content Filtering

Attachment Filtering

bitdefender
secure your every bit

BitDefender Security for Exchange

User's guide

BitDefender

Published 2007.06.20
Version 2.0

Legal Notice


bitdefender
secure your every bit

Table of Contents

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.

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>.

About BitDefender

1. Who is BitDefender?

BitDefender is a leading global provider of security solutions that satisfy the protection requirements of today's computing environment. The company offers one of the industry's fastest and most effective lines of security software, setting new standards for threat prevention, timely detection and mitigation. BitDefender delivers products and services to over 41 million home and corporate users in more than 180 countries. BitDefender has offices in the **United States**, the **United Kingdom**, **Germany**, **Spain** and **Romania**.

- Features antivirus, firewall, antispyware, antispam and parental control for corporate and home users;
- The BitDefender range of products is intended to be implemented on complex IT structures (work stations, file servers, mail servers, and gateway), on Windows, Linux and FreeBSD platforms;
- Worldwide distribution, products available in 18 languages;
- Easy to use, with an installation wizard that guides users through the installation process and only asks a few questions;
- Internationally certified products: Virus Bulletin, ICSA Labs, Checkmark, IST Prize, etc;
- Round the clock customer care – the customer care team is available 24 hours, 7 days a week;
- Lightning fast response time to new computer attacks;
- Best detection rate;
- Hourly Internet updates of virus signatures - automatic or scheduled actions offering protection against the newest viruses.

1.1. Why BitDefender?

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

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

Comprehensive. Covers every single point of your network, providing complete security. BitDefender security solutions for the corporate environment satisfy the protection requirements of today's business environment, enabling management of all complex threats that endanger a network, from a small local area to large multi-server, multi-platform WAN's.

Your Ultimate Protection. The final frontier for any possible threat to your computer system. As virus detection based on code analysis has not always offered good results, BitDefender has implemented behavior based protection, providing security against newborn malware.

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

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

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

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

Further information about BitDefender can be obtained by visiting: http://www.bitdefender.com.

Product Installation

2. BitDefender Security for Exchange Installation

2.1. System Requirements

Before installing the product, make sure that your system meets the following minimum system requirements:

Software

- Internet Explorer 6
- Exchange 2003 Standard or Enterprise or
- Exchange 2000 Standard or Enterprise SP1 or
- Exchange 5.5 SP3 + Windows NT 4.0 SP6 + MMC v1.2 / Windows 2000 SP4

Hardware

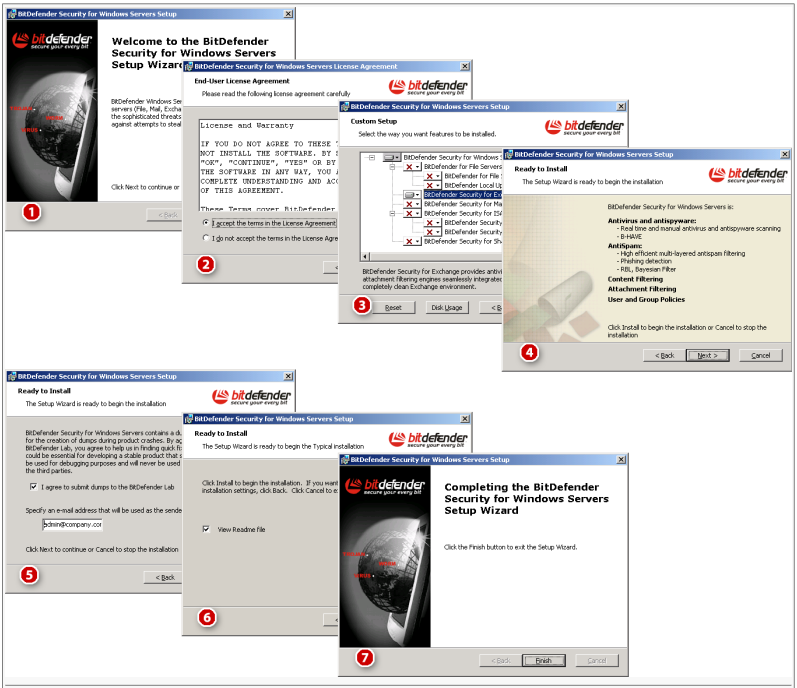
- Minimum Processor - Pentium II 300 MHz
- 128 megabytes (MB) of RAM, 256 MB recommended or 256 megabytes (MB) of RAM, 512 MB recommended for Exchange 2003
- Minimum hard disk space - 100MB (instalation only)

2.2. Installing the Product

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

Before launching the setup wizard, BitDefender will check for newer versions of the installation package. If a newer version is available, you will be prompted to download it. Click **Yes** to download the newer version or **No** to continue installing the version then available in the setup file.

BitDefender will also check if BitDefender Security for Exchange is already installed on the local computer. If the same version as the one in the setup file is installed, you will have to modify the existing configuration. If an older version is installed, the installation process will continue as it should, with the only difference that the already installed products will be re-installed (upgraded) by default.



Installation Steps

Follow the next steps to install BitDefender Security for Exchange:

1. Click **Next** 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 to these terms click **Cancel**. The installation process will be abandoned and you will exit setup.
3. You can see the list of all BitDefender products designed for Windows-based servers.

   Select BitDefender Security for Exchange, click the corresponding **arrow** and then click **Will be installed on local hard drive** on the shortcut menu.

Note

You can also install other BitDefender products for Windows-based servers. Select them as shown before. The items marked with a red cross will not be installed.

Click **Next**.

Note

If BitDefender does not detect an MS Exchange Server installed on the local computer, an error message will appear and the installation process will be cancelled. Click **OK&Finish** to exit the wizard.

4. Click **Next**.
5. BitDefender Security for Exchange contains a dump management module that allows creating dumps during product crashes. By agreeing to send the dumps to the BitDefender Lab, you agree to help us find quick fixes for our bugs. You could make a major contribution to the development of a stable product that satisfies your needs. The dumps will only be used for debugging purposes. They will never be used as commercial data or disclosed to third parties.

   To send dumps to the BitDefender Lab, check **I agree to submit dumps to the BitDefender Lab** and specify your e-mail address.

   Click **Next**.
6. Check **View Readme file** if you want to open the readme file at the end of the installation.

   Click **Install** in order to begin the installation of the product.

   Note

   BitDefender will automatically detect your version of Microsoft Exchange Server.

7. Click **Finish** to complete product installation.

   Note

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

2.3. Uninstalling or Repairing BitDefender

If you want to modify, repair or remove **BitDefender Security for Exchange**, follow the path from the Windows start menu: **Start → Programs → BitDefender Security for Exchange → Modify, Repair or Uninstall**.

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

- **Modify** - to select new BitDefender products for Windows-based servers to add or to select such currently installed products to remove.
- **Repair** - to re-install the product.

Important

Before repairing the product we recommend you to export the console settings and the settings lists where possible (i.e. White / Black lists, Allow / Deny IP list, Sender Blacklist). After the repair process is over you may reload them.

- **Remove** - to remove all installed components.

To continue setup, select either of the options listed above. We recommend that you choose **Remove** for a clean re-installation.

Description and Features

3. BitDefender Security for Exchange

Comprehensive protection for Exchange Servers

BitDefender Security for Exchange provides antivirus, antispyware, antispam, antiphishing, attachment and content filtering seamlessly integrated with the MS Exchange Server, to create a malware free messaging environment. It protects Exchange servers against the latest most sophisticated malware and against attempts to steal users' confidential and valuable data.

Note

With MS Exchange 5.5 only antivirus protection is provided. For other features, we recommend using it together with BitDefender Security for Mail Servers.

3.1. Key Benefits

- Increased productivity
- Reduced mail traffic
- E-mail protection against a wide range of malware
- High stability
- Ease of use and management
- Low resource/network impact

3.2. Key Features

- Superior antivirus protection
- Proactive heuristic protection against zero-day threats
- Multiple layers of anti-spam filtering
- Content and attachment filtering
- Antispyware and antiphishing protection
- Detailed reports and statistics
- Intuitive program interface
- Centralized management software compatibility

3.3. BitDefender Advanced Technologies

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

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

NeuNet Filter. To better deal with new spam, the BitDefender Lab has created NeuNet, a powerful antispam filter. Inside the Antispam Lab, NeuNet is pre-trained on a series of spam messages so that it learns to recognize new spam by perceiving its similarities with the messages it has already examined.

Certified Antivirus Engines. BitDefender's award winning scan engines featuring the B-HAVE technology have been recognized by ICSA Labs, Virus Bulletin and Checkmark to provide the most proactive antivirus protection available.

3.4. Core Functionalities

Blocks Infected Messages. BitDefender Security for Exchange fights e-mail-borne malware by filtering and blocking messages that carry a virus, spyware, Trojan, backdoor or other potentially dangerous active codes.

Optimized for Exchange. The product is deeply integrated with MS Exchange using its VSAPI technology. It offers advanced e-mail filtering without affecting server performance or the e-mail traffic.

Enhanced Protection. Organizations with several mail servers can have a gateway server that receives mail directly from the Internet and distributes it to the other servers. Messages routed by the gateway Exchange Server 2003 are scanned at transport level by BitDefender Security for Exchange so that the mail reaching users of the internal servers is free from malware. As a result, internal server resources are saved and the entire messaging environment is provided with an additional defense layer.

Safe Messaging Environment. The SMTP Service integrated filter blocks threats before they can enter/leave the Exchange server. Mails are scanned at the point they enter/leave the server so that the messaging environment is free from malware at all times. This type of protection has a wider span as it also keeps the external recipients of the filtered mail (customers, partners, friends) safe from malware. The product is

light on mail server resources and the inbound or outbound mail traffic poses no threat at all for the messaging environment of your company or of your partners' company.

Highly Efficient Antispam Filtering. Connection and protocol filters such as the Allow/Deny IP List and Sender Black List are just two instances of the product's multi-layered antispam protection system. E-mails that pass first level filters undergo content analysis at the central dispatcher, which decides what product filters to use so as to accurately classify messages as spam, phishing or legitimate.

Proactive Phishing Detection. The anti-phishing technology detects illegal attempts to copy the "look and feel" of authentic messages intended to trick the user into sending confidential data to a particular recipient.

Spyware protection. A comprehensive signature database and heuristic spyware detection help protect against spyware and avoid the theft of confidential and valuable data.

WBL (White List/ Blacklist) Support. The administrator can set a list of trusted and untrusted addresses based on which to respectively "always accept" or "always reject" mail.

Real-time Blackhole List Filter. The RBL filter identifies spam based on mail servers' reputation as spam senders.

Bayesian Antispam Filter. Users can train the Bayesian Filter to identify spam by allowing it to learn to discern between spam and legit mail based on specific examples from their mailboxes.

Configurable Antispam Filter Sensitivity. The administrator can adapt the antispam filter's sensitivity by setting very demanding or relaxed thresholds for each user group.

IP Match. E-mails with spoofed headers no longer fool the White List filter because each e-mail domain is matched to a particular IP address so that messages with non-matching IP addresses are rejected.

Automatic Redirection of Spam to Junk Folder. The Exchange SCL integration along with MS Intelligent Message Filter allows spam mails to be redirected to the Exchange 2003 user's Junk Folder.

Content and Attachment Filtering. A set of rules can be configured to prevent malicious and offensive content/attachments from entering the company.

User and Group Policies. Antivirus, antispam, content and attachment filtering policies can be defined for different users and groups, allowing system administrators to filter mail traffic in a more flexible manner.

3.5. Increased Usability

Reports and Statistics. A comprehensive database related to the product's activity allows generating detailed statistics and reports to help system administrators monitor the mail server.

Remote Management. Server protection can be remotely configured by simply installing the management console on one computer inside the network.

Centralized Management. BitDefender Security for Exchange is compatible with BitDefender Enterprise Manager, allowing organizations to centrally manage antivirus protection and security policies inside complex networks.

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

Quarantine Management. Dangerous or restricted mails going through the antivirus, antispam, content and attachment filtering modules can be isolated in a quarantine zone where the system administrator can deal with them at will.

3.6. Services

Advanced Update System. For permanent server protection, the product receives the latest updates and patches based on four configurable technologies: on-demand, scheduled, automatic and pushed.

Update Pushing. The latest virus signatures are "pushed" to your servers the second they become available instead of waiting for the next scheduled update, further reducing the threat presented by new viruses.

Product Update. Product fixes and enhancements can be downloaded automatically. Alerts are sent upon the release of new versions and the administrator can decide when to install them.

Upgrades. Registered users benefit from free upgrades to any new version of the product during the license period. Special price offers are also available to returning customers.

Free 24/7 Professional Technical Support. Certified representatives provide BitDefender business customers with free permanent support online, by telephone or e-mail. This is supplemented by an online database with answers to Frequently Asked Questions and fixes for common issues.

4. Core Modules

The core functionalities of **BitDefender Security for Exchange** are defined by 4 modules: **Antivirus**, **Antispam**, **Content Filtering** and **Attachment Filtering**.

4.1. Antivirus Module

BitDefender protects the Exchange server from viruses, spyware and other malware by scanning the messages in users' mailboxes and the objects in public folders upon clients' request. The MS Exchange mail server was designed with a low level interface, VS API, intended to offer antivirus scanning support. This interface also allows scanning messages with multiple recipients once, before delivery, instead of many times, for each mail receiver separately. BitDefender deeply integrates with this interface.

Different scanning policies can be defined for users and user groups. The rules are those that specify the antivirus scanning settings and the actions to take on the infected messages, based on the groups to which the sender and the receivers belong.

Besides the classic on-access scanning, the message can also be scanned before the client's request, regardless of the existing rules. This can be done through several additional scanning methods, intended to optimize the overall scanning process: background, proactive and transport scanning.

4.1.1. Background Scanning

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

To perform background scanning of the messages and attachments, the Information Store will use one thread per database, running at low priority. Once the background scanning is completed, the thread is terminated. This thread is not part of the global virus-scanning thread pool used for on-access scanning.

4.1.2. Proactive Scanning

Proactive scanning means that 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 threads are available in the thread pool and no high priority item remains to be scanned, each low priority item is submitted for scanning.

If an item is on the low priority list and a client attempts to access the message, the item will be marked as high priority. Also, it will be removed from the low priority list and another low priority item will take its place.

4.1.3. Transport Scanning

Note

Transport scanning is available only on MS Exchange Server 2003!

Transport scanning means that messages are scanned at the transport level. This prevents infected messages from entering the Exchange organization.

The messages entering the Exchange store are intercepted by the VS API interface and scanned by BitDefender. After being scanned, the messages are submitted again to the transport engine which will deliver them to their destination. Any message scanned at the gateway will be rescanned on the back-end server.

Note

We recommend enabling transport scanning only when BitDefender Security for Exchange is installed on a gateway.

4.2. Antispam Module

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

Different filtering policies can be defined for users and user groups. The rules are those that specify which filters to use to analyze the message and the actions to take on spam, based on the groups to which the sender and the receivers belong.

The Antispam filters are grouped into two categories:

- **Global filters** - configurable filters meant to filter all incoming mail traffic, regardless of the policies set.

Note

The Real-time Blackhole List (RBL) filter can be deactivated in policies.

- **Policy filters** - filters applied to the incoming mail traffic according to the specified policies.

4.2.1. Global Filters

There are 4 global filters: Allow / Deny IP List, Sender Black List, IP Match and Real-time Blackhole List.

Note

These filters must be configured globally by the administrator. In order to configure them, go to the **Antispam** module, Antispam section and click **Global Filters**. For more details, please refer to "*Configuring Global Antispam Filters*" (p. 138).

Allow / Deny IP List

The Allow / Deny IP List enables the administrator to specify IP addresses which are denied access to the server. All incoming connections from addresses that appear on the Deny IP List are dropped, provided that such addresses do not appear on the Allow IP List.

Note

The Allow IP List is used to except IP addresses from ranges of IP addresses defined on the Deny IP List.

Sender Black List

The Sender Black List allows the administrator to specify a list of e-mail addresses which are denied access to the server. The incoming mail from these addresses will be dropped before reaching the server.

IP Match

Spammers often try to "spoof" the sender's e-mail address to make the e-mail appear as being sent by someone in your domain. To prevent this, you can use IP Match.

If a message appears to be from a domain that you have specified in the IP Match rule list (such as your own company domain), BitDefender checks to see if the IP address of the sender matches one of the IP addresses provided for the specified domain. If the domain address of the sender matches an associated IP address, the message is considered legitimate and antispam filtering stops. Otherwise, the message is considered SPAM and the connection is dropped.

Real-time Blackhole List

The Real-time Blackhole List (RBL) filter allows checking the mail server from which a message is sent against the RBL servers configured by the administrator. It uses

the DNSBL protocol and RBL servers to filter spam based on mail servers' reputation as spam senders.

The mail server address is extracted from the e-mail header and its validity is checked. If the address belongs to a private class (`10.0.0.0`, `172.16.0.0` to `172.31.0.0` or `192.168.0.0` to `192.168.255.0`) or it is not relevant, it will be ignored.

A DNS check is performed on the domain `d.c.b.a.rbl.example.com`, where `d.c.b.a` is the reversed IP address of the server and `rbl.example.com` is the RBL server. If the DNS replies that the domain is valid, it means that the IP is listed in the RBL server and a certain server score is provided. This score ranges between 0 and 100, according to the configured server confidence (trust level).

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

If the RBL filter score is 100 or higher, the message is considered SPAM and the specified action is taken. Otherwise, a spam score is computed from the RBL filter score and added to the global spam score of the message.

Note

The RBL filter can be deactivated under certain policies.

4.2.2. Policy Filters

There are 8 policy filters: White List / Black List, Block sexually explicit content, Charset filter, URL filter, Image filter, Bayesian filter, Pre-trained Bayesian filter and NeuNet (Heuristic) filter.

Note

These filters can be enabled and configured by the administrator separately for each rule. In order to configure them, go to the **Antispam** module, Policies section and set the appropriate rules. For more details, please refer to "*Creating Rules*" (p. 147).

White List / Black List

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

Note

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

The filter is highly flexibile as it can be configured separately for different groups of users. Note that the lists must be configured for each rule in order to apply the filter to the corresponding incoming mail traffic.

Block Sexually Explicit Content

This filter detects messages marked as `SEXUALLY-EXPLICIT:` in the subject line and tags them as SPAM.

Note

Starting May 19, 2004, spam that contains sexually oriented material must include the warning `SEXUALLY-EXPLICIT:` in the subject line or face fines for violations of federal law.

Charset Filter

Many spam messages are written in Cyrillic and / or Asian charsets. The Charset Filter detects this kind of messages and tags them as SPAM.

URL Filter

Almost all spam messages include links to various web locations. These locations usually contain more advertising and the possibility to buy things, and, sometimes, they are used for phishing.

BitDefender maintains a database of such links. The URL filter checks every URL link in a message against its database. If a match is made, the message is tagged as SPAM.

Image Filter

Since avoiding heuristic filter detection has become quite a challenge, images are increasingly used in spam messages. Many spam messages contain either a single spam image or a spam image and a random text meant to deceive the heuristic filter.

The Image filter deals with image spam. It compares the image from a message with those from the BitDefender database. In case of a match, the message is tagged as SPAM.

Bayesian Filter

The Bayesian filter is the trainable component of the Antispam module. It constantly collects statistical information about server-specific spam and legitimate messages provided by the administrator and it analyzes messages according to this information

This information refers to the rate at which specific words appear in messages classified SPAM as compared to those declared NON-SPAM. This means, for example, that if a certain four-letter word is seen to appear more often in SPAM, it will be naturally presumed that it is very likely for the next incoming message including this word to actually be SPAM. All relevant words within a message are taken into account. By synthesizing the statistical information, the overall probability for the whole message to be SPAM is computed and a SPAM score is added to the message.

Pre-trained Bayesian Filter

While the Bayesian filter is trained on server-specific messages, this filter is pretrained by the BitDefender Antispam Lab on our own database of spam and legitimate messages and updated periodically.

NeuNet (Heuristic) Filter

The NeuNet (Heuristic) filter performs a set of tests on all 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. Based on the results of the analysis, it adds a SPAM score to the message.

4.3. Content Filtering Module

The Content Filtering module prevents malicious or offensive mail content from entering the Exchange server mailboxes.

Content Filtering checks messages to see if the subject, the sender's or the receiver(s)' address contain certain specified strings. If a defined string matches one of these mail headers, the message is detected and the specified action is taken.

Different filtering policies can be defined for users and user groups. The rules are those that specify the filtering settings and the actions to be taken on the messages that match the rule, based on the groups to which the sender and the receivers belong.

4.4. Attachment Filtering Module

The Attachment Filtering module prevents potential malicious or large attachments from entering the Exchange server mailboxes.

Attachment Filtering checks mail attachments to see if their name matches certain patterns, if they have a different extension than those specified or if they exceed a certain size limit. In any of these cases, the message containing the respective attachment is detected and the specified action is taken.

Different filtering policies can be defined for users and user groups. The rules are those that specify the filtering settings and the actions to be taken on the messages that match the rule, based on the groups to which the sender and the receivers belong.

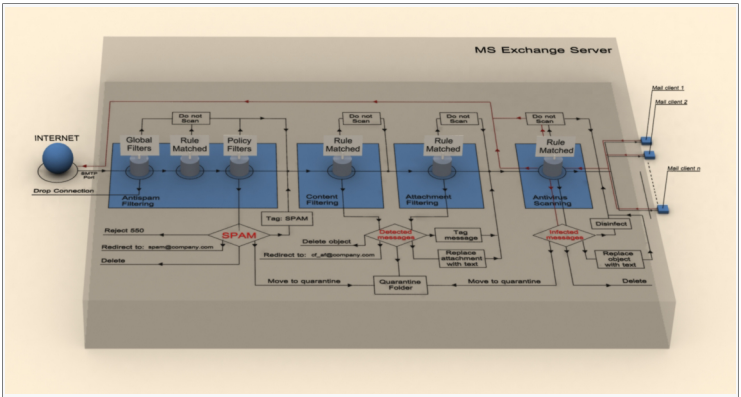
5. How Does It Work?

BitDefender checks mail using antispam, then content and attachment filtering and finally antivirus scanning. This keeps clients' Inboxes free of spam, phishing attempts, viruses and spyware and other unwanted content.

Note

For Microsoft Exchange 5.5, only antivirus scanning is performed on messages.

The diagram below shows how BitDefender works:



Working Schema

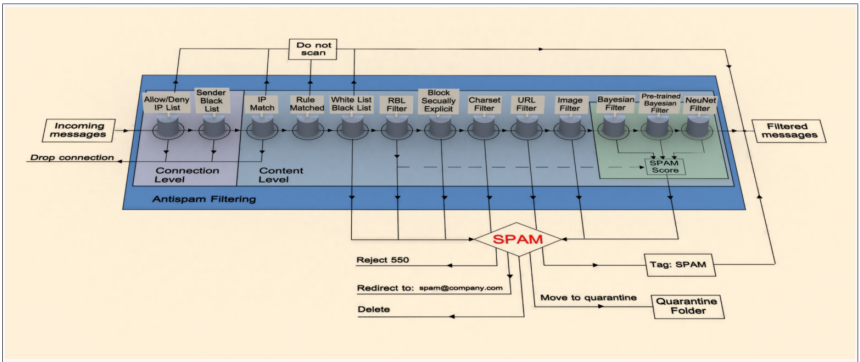
Lets consider that all the filters and engines are enabled and see how BitDefender filters the mail traffic. A message is verified, in the following order, by:

1. Antispam Filtering
2. Content Filtering
3. Attachment Filtering
4. Antivirus Scanning

5.1. Antispam Filtering

The Antispam module will check the message first. Antispam filtering works at both connection and content level to ensure efficient protection against spammers and less traffic on the server.

The diagram below shows how antispam filtering works:



Antispam Filtering

Note

For detailed information about the Antispam filters, check the description of the Antispam Module.

5.1.1. Connection Level

When an attempt is made to establish a connection, the message is checked against the **Allow / Deny IP List**. If there is a match, the connection is dropped.

Otherwise, the message is checked against the global **Sender Black List**. If the filter finds a match, the connection is dropped.

5.1.2. Content Level

If the message passes connection level filters, it is unpacked and filtered at content level.

First, the message is checked against the **IP Match** filter. If a match is found, there are two possibilities:

- the message is considered legitimate and antispam filtering stops.
- the connection is dropped.

If the message does not match the IP Match filtering criteria, it is then checked based on a specific **antispam filtering group policy**.

The message is checked against the antispam filtering rules, by order of priority, until the sender and the receivers of the message match a rule. The message is then processed according to the options specified by that rule.

- If the action set for the rule is **Do not scan**, the antispam filtering stops.
- If the action set for the rule is **Scan**, several antispam filters will take over the message in the following order:
  1. **G-Tube.** If the message matches the G-Tube test, it is considered SPAM, the antispam filtering stops and the specified action is taken on the message.
  2. **White List / Black List Filter.** If a match is found against the White List, the filtered message is considered legitimate and the antispam filtering stops. If a match is found against the Black List, the filtered message is considered SPAM, the antispam filtering stops and the specified action is taken on the message.
  3. **Real-time Blackhole List (RBL).** The filter analyzes the message and, if matches are found, modifies its SPAM score. If the SPAM score exceeds a certain value, the message is considered SPAM, the antispam filtering stops and the specified action is taken on the message.
  4. **"Block sexually explicit content" Filter.** If the message matches the filtering rule, it is considered SPAM, the antispam filtering stops and the specified action is taken on the message.
  5. **Charset Filter.** If the message matches the filtering rule, it is considered SPAM, the antispam filtering stops and the specified action is taken on the message.
  6. **URL Filter.** If a match is found against the filter's database, the filtered message is considered SPAM, the antispam filtering stops and the specified action is taken on the message.
  7. **Image Filter.** If a match is found against the filter's database, the filtered message is considered SPAM, the antispam filtering stops and the specified action is taken on the message.
  8. **Bayesian Filter.** The filter analyzes the message and modifies its SPAM score.
  9. **Pre-trained Bayesian Filter.** The filter analyzes the message and modifies its SPAM score.

10. **NeuNet(heuristic) Filter.** The filter analyzes the message and modifies its SPAM score.

After the last filter checks the message, the SPAM score is compared to the threshold level specified for the rule that is applied. If the final SPAM score exceeds the threshold level, then the message is considered SPAM and the specified action is taken. Otherwise, the message is allowed to pass without any action taken.

5.2. Content Filtering

If the message is not deleted during antispam filtering, it is then verified according to a specific **content filtering group policy**.

The message is checked against the content filtering rules, by order of priority, until the sender and the receivers of the message match a rule. The message is then processed according to the options specified by that rule.

- If the filtering option set for the rule is **Do not scan**, the message is not processed using content filtering.
- If the filtering option set for the rule is **Scan**, the message is checked according to the content filtering options specified by the rule. If the message matches the rule, the content filtering stops and the specified actions are taken on the message. Otherwise, the message is allowed to pass without any action taken.

5.3. Attachment Filtering

If the message is not deleted during content filtering, then the mail attachments, if any, are verified according to a specific **attachment filtering group policy**.

The message is checked against the attachment filtering rules, by order of priority, until the sender and the receivers of the message match a rule. The message is then processed according to the options specified by that rule.

- If the option set for the rule is **Do not scan**, the message is not processed using attachment filtering.
- If the filtering option set for the rule is **Scan**, the message is checked according to the attachment filtering options specified by the rule. If the message matches the rule, the attachment filtering stops and the specified actions are taken on the message. Otherwise, the message is allowed to pass without any action taken.

5.4. Antivirus Scanning

If the message reaches the Exchange store, it is scanned for viruses and spyware when the client requests it, according to a specific **antivirus scanning group policy**.

The message is checked against the antivirus scanning filtering rules, by order of priority, until the sender and the receivers of the message match a rule. The message is then processed according to the options specified by that rule.

- If the filtering option set for the rule is **Do not scan**, the message is not scanned for malware.
- If the scan option set for the rule is **Scan**, the message is checked according to the scanning options specified by the rule. If the message is found infected, the scanning stops and the specified actions are taken on the message. Otherwise, the message is allowed to pass without any action taken.

Besides the classic on-access scanning, the message can also be scanned before the client's request, regardless of the existing rules. This can be done through several additional scanning methods, intended to optimize the overall scanning process: background, proactive and transport scanning.

This is how scanning works:

- If the message was not scanned before the client's request, it is scanned according to the rule.
- If the message was checked before by proactive or background scanning and no update was performed in the meantime, the message is delivered without being scanned according to the rule.
- If the message was checked before by proactive or background scanning but an update was performed in the meantime, the message is scanned according to the rule.
- Only for MS Exchange Server 2003! If the message was previously scanned at transport level, it is also scanned according to the rule.

Configuration and Use

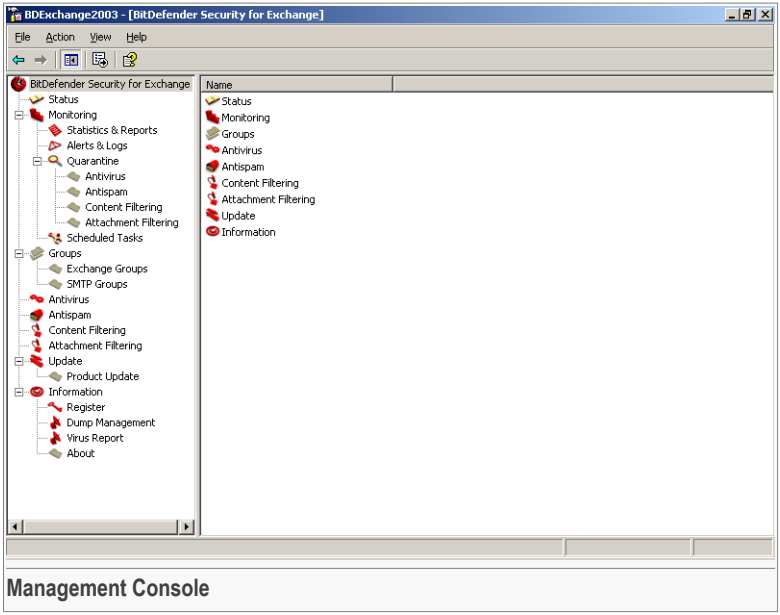
6. Overview

BitDefender Security for 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 new **BitDefender Security for Exchange** comes with an MMC-based interface which improves user experience.

6.1. Getting Started

To access the management console, use the Windows Start menu, by following the path **Start → Programs → BitDefender Security for Exchange → BitDefender Security for Exchange**.



Management Console

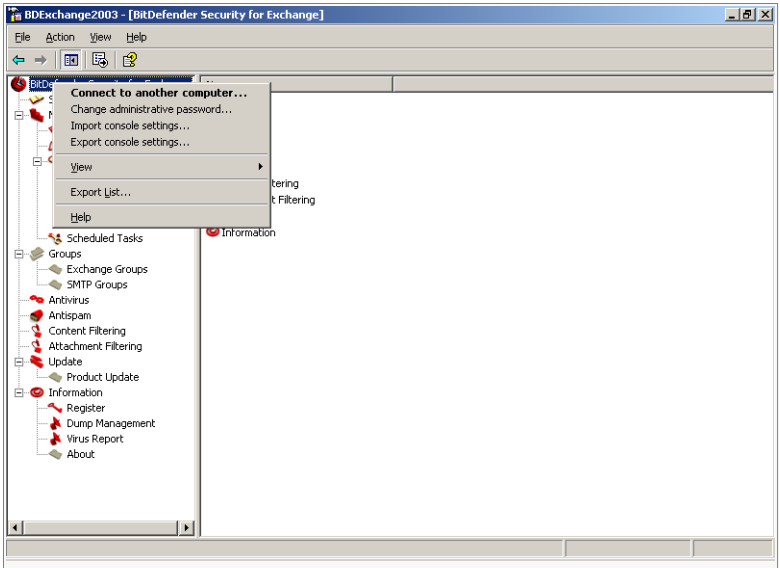
On the left side of the management console you can see the tree menu:

- Status - provides essential information about the product (product, modules and update status). Here, you can also enable or disable the BitDefender scanning and filtering modules.
- Monitoring - contains sections that allow you to monitor the product activity.
  - Statistics & Reports - offers complete information on the product activity. You can analyze detailed statistics and create customized reports on the product activity.
  - Alerts & Logs - allows configuring file logging and sending alerts for certain events that occur, such as an update error or an infected file detected.
  - Quarantine - stores detected files, grouped into four categories (Antivirus, Antispam, Content Filtering, Attachment Filtering).
  - Scheduled Tasks - allows creating scheduled tasks through an intuitive wizard. You can schedule updates, on-demand and background scanning processes and reports to be generated.
- Groups - provides group management.
  - Exchange Groups - this is where you can configure and manage the Exchange user groups.
  - SMTP Groups - this is where you can configure and manage the SMTP user groups, based on Active Directory.
- Antivirus - this is where you can configure the **Antivirus** module.
- Antispam - this is where you can configure the **Antispam** module.
- Content Filtering - this is where you can configure the **Content Filtering** module.
- Attachment Filtering - this is where you can configure the **Attachment Filtering** module.
- Update - this is where you can configure the **Update** module.
  - Product Update - this is where you can check if upgrades are available and install them.
- Information - contains sections where global settings are configured and general information is provided.
  - Register - this is where you can register the product.
  - Dump Management - this is where you can allow BitDefender to send dumped items to the BitDefender Lab.
  - Virus Report - this is where you can enable virus reporting.
  - About - shows product details.

If you want to open the help file, click **Help -> About BitDefender Security for Exchange**. A contextual help is available for each window. Click ? to open it.

6.2. Contextual Menu

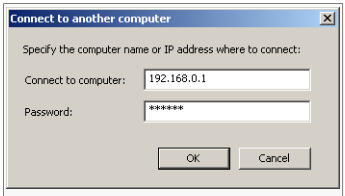
Right-click **BitDefender Security for Exchange** to open the contextual menu.



Contextual Menu

Four options are available on the contextual menu:

- **Connect to another computer** - opens a window where you can specify the name or the IP of the server to which you want to remotely connect and the administrative password of the product that you want to manage.



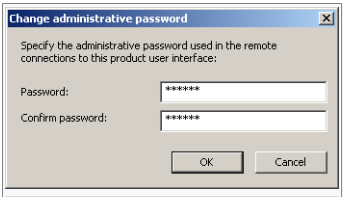
Connect to another computer

Type the server name or IP in the **Connect to computer** field and the password in the **Password** field.

Click **OK**.

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

- **Change administrative password** - opens a window where you can specify the administrative password for BitDefender Security for Exchange. This password will be used when connecting remotely to this interface.



Change administrative password

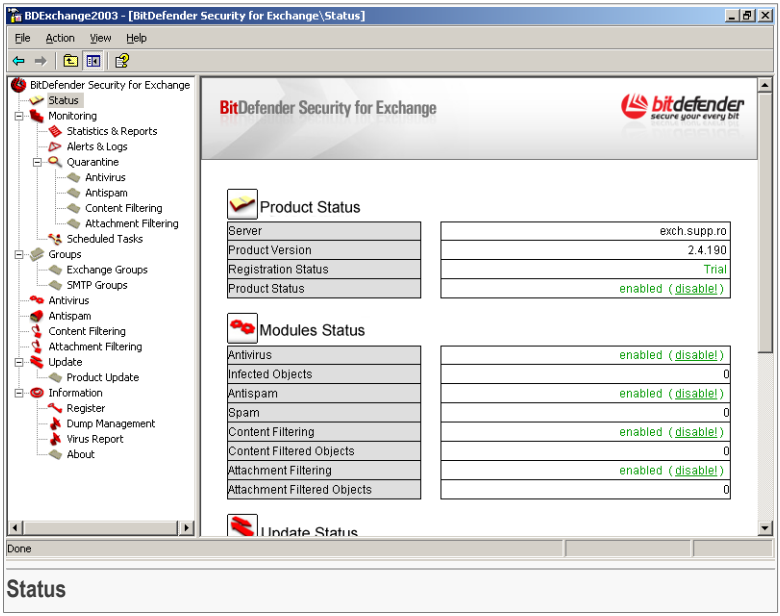
Type the password in the **Password** field and re-type it in the **Confirm password** field.

Click **OK**.

- **Import console settings** - imports previously saved console settings.
- **Export console settings** - exports the console settings to a txt file.

7. Status Module

Click **Status** in the tree menu to enter this section.



This is where you can view information about the status of the BitDefender modules and you can enable / disable them.

In order to easily monitor product activity, BitDefender uses two colors: green and red. The green color means that all is ok, while the red color indicates that the corresponding item requires your attention.

The information is grouped under three headings:

- **Product Status** - indicates whether the product is enabled or disabled and allows you to change the product status. Also, this is where you can see the server name, the product version and the registration status.

  If you want to quickly enable / disable BitDefender click the corresponding link. This will apply to all the modules under the **Modules Status** heading.

- **Modules Status** - provides status information about the BitDefender scanning and filtering modules: Antivirus, Antispam, Content Filtering and Attachment Filtering. Below the status of each module you can see the number and the percentage, respectively, of infected files, spam messages, files that match the content and attachment filtering rules, since installation or since when you last cleared the records.

  Click the corresponding link to enable / disable a BitDefender component.

- **Update Status** - provides update-related information and alerts you whenever a product update is available. You can see when the last check for updates and the last update were performed as well as the number of available virus signatures.

8. Monitoring Module

Click **Monitoring** in the tree menu to enter this section.

Monitoring

This is where you can monitor the product activity.

The **Monitoring** module contains the following sections:

- Statistics & Reports - offers statistic information about the product activity and allows creating customized reports based on the statistics and on the log file.
- Alerts & Logs - allows configuring events, such as a failed update or an infected file detected, to be notified by mail or net send or to be logged in the BitDefender log file.
- Quarantine - shows the files and mails stored in the quarantine folder. These objects were found infected or suspect, detected as spam, or matched a content or an attachment filtering rule and were moved to the quarantine folder according to the specified action. They are grouped into four categories (Antivirus, Antispam, Content

Filtering, Attachment Filtering), based on the BitDefender component that detected them.

- Scheduled Tasks - allows creating scheduled tasks through an intuitive wizard. You can schedule updates, on-demand and background scanning processes and reports to be generated.

In this chapter, you can find a detailed description of each section.

8.1. Statistics & Reports

The **Statistics & Reports** module offers the possibility to obtain statistic data regarding the product activity since the last installation or the last time the records were cleared.

The module contains two sections:

- Statistics - provides real-time statistic information regarding the activity of the Antivirus, Antispam, Content and Attachment Filtering modules, both separately and as a whole.
- Reports - allows generating customized reports based on the BitDefender statistics and on the log file.

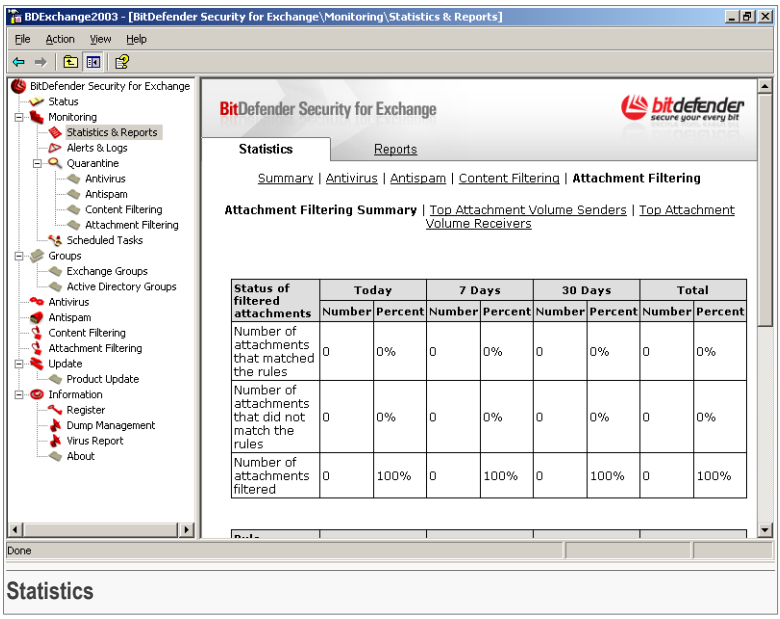
Note

If you right-click **Statistics & Reports** on the tree menu, a shortcut menu will appear.

- To delete all data regarding the product activity, select **Clear all records**. Please note that clearing all records will affect both statistics and reports.
- To run the report wizard to create a new report, select **New Report**.

8.1.1. Statistics

Click **Statistics & Reports** in the tree menu (**Monitoring** module) to enter this section.



Statistics

This is where you can find valuable information regarding the activity of BitDefender Security for Exchange.

Note

The **Statistics** window is refreshed every 60 seconds in order to provide you with real-time information.

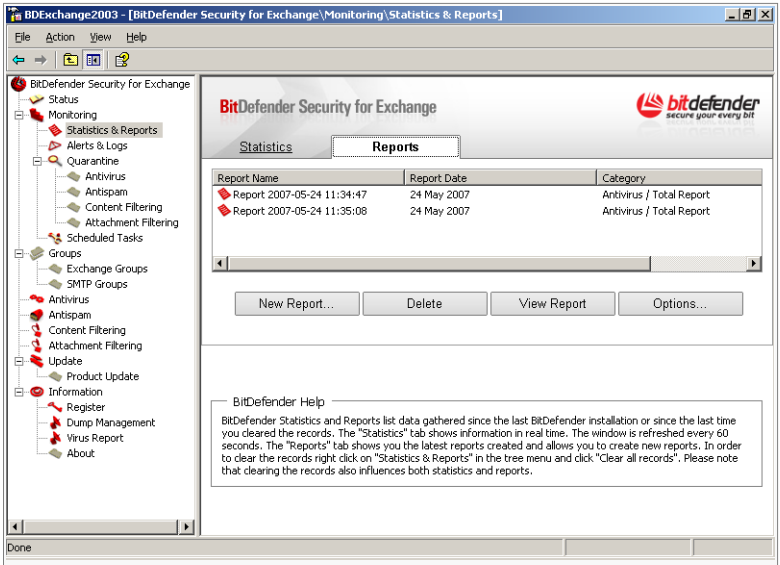
There are five main windows which provide real-time statistic information on the overall product activity and the activity of the Antivirus, Antispam, Content Filtering and Attachment Filtering modules. Each of these categories contains several types of statistics grouped into 4 time intervals: present day, last week, last month and total. Click a link to access the corresponding statistics.

The following types of statistics are available:

Category	Type	Description
Summary		Provides overall statistics on the activity of BitDefender Security for Exchange.
Antivirus		Contains the statistics on the Antivirus module.
	Antivirus Summary	Provides overall statistics on the activity of the Antivirus module.
	Top Viruses	Shows the top of the viruses detected.
	Top Virus Senders	Lists mail senders based on the number of viruses sent.
	Top Virus Receivers	Lists mail receivers based on the number of viruses received.
Antispam		Contains the statistics on the Antispam module.
	Antispam Summary	Provides overall statistics on the activity of the Antispam module.
	Top Spam Senders	Lists mail senders based on the spam volume sent.
Content Filtering		Contains the statistics on the Content Filtering module.
	Content Filtering Summary	Provides overall statistics on the activity of the Content Filtering module.
	Top Content Volume Senders	Lists mail senders based on the number of content filtering rules matched.
	Top Content Volume Receivers	Lists mail receivers based on the number of content filtering rules matched.
Attachment Filtering		Contains the statistics on the Attachment Filtering module.
	Attachment Filtering Summary	Provides overall statistics on the activity of the Attachment Filtering module.
	Top Attachment Volume Senders	Lists mail senders based on the number of attachment filtering rules matched.
	Top Attachment Volume Receivers	Lists mail receivers based on the number of attachment filtering rules matched.

8.1.2. Reports

Click **Statistics & Reports** in the tree menu (**Monitoring** module) and then the **Reports** tab to enter this section.



Reports

This is where you can create customized reports on the product activity based on the statistics and on the log file. Here you can also manage and view reports.

Reports provide information about the activity of the Antivirus, Antispam, Content Filtering and Attachment Filtering modules. They contain general information (the report name, the time interval for which the report is generated and the server name) and specific information which depends on the type of report. Reports can be generated in HTML, text or comma-separated values (CSV) format.

The following types of reports are available:

Module	Report Type	Description
Antivirus	**Total**	Provides complete information on the activity of the Antivirus module.

Module	Report Type	Description
	Top Viruses	Provides a table containing the viruses detected, in descending order.
	Top Virus Senders	Contains the mail senders ordered by the number of viruses sent.
	Top Virus Receivers	Contains the mail receivers ordered by the number of viruses received.
Antispam	**Total**	Provides complete information on the activity of the Antispam module.
	Top Spam Senders	Contains the mail senders ordered by the spam volume sent.
Content Filtering	**Total**	Provides complete information on the activity of the Content Filtering module.
	Top Content Volume Senders	Contains the mail senders ordered by the number of content filtering rules matched.
	Top Content Volume Receivers	Contains the mail receivers ordered by the number of content filtering rules matched.
Attachment Filtering	**Total**	Provides complete information on the activity of the Attachment Filtering module.
	Top Attachment Volume Senders	Contains the mail senders ordered by the number of attachment filtering rules matched.
	Top Attachment Volume Receivers	Contains the mail receivers ordered by the number of attachment filtering rules matched.

Managing Reports

You can see all the existing reports listed in the table. For each report, the following information is provided: the report name, the date when the report was generated, the type of information it contains and the format.

To manage the reports, use these buttons:

- **New Report** - launches a wizard that will help you create a new report.
- **Delete** - deletes one or several selected report files. You will have to confirm your choice by clicking **Yes**.
- **View Report** - opens a selected report file.

Note

To open a report file you can also double-click it.

- **Options** - opens a new window where you can specify how long report files should be kept. Enter the number of hours / days / weeks / months during which to store reports and click **OK** to save changes.

Note

Reports older than the specified period will be automatically deleted.

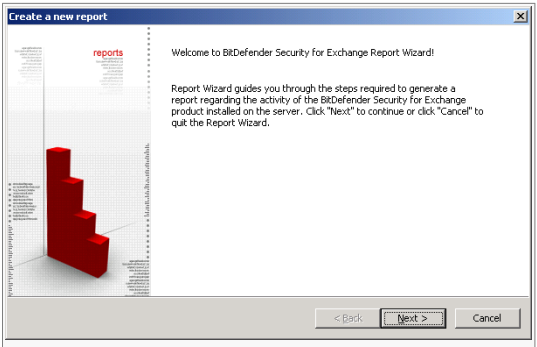
Creating Reports

To create report files on the product activity conducted over a certain period of time, click **New Report**. The report wizard will appear. This is a five step procedure, which will help you generate report files.

Note

To run the wizard, you can also right-click **Statistics & Reports** in the tree menu and then click **New Report** in the contextual menu.

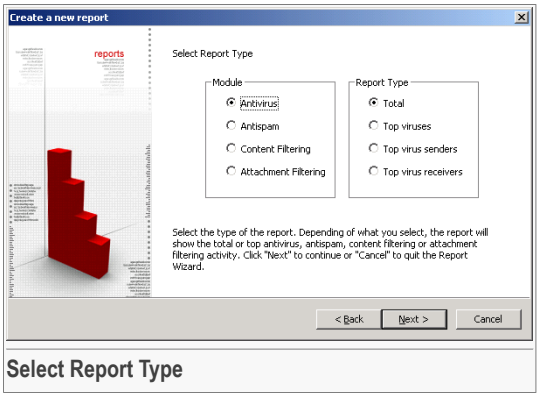
Step 1/5 - Welcome to the Report Wizard



Welcome

Click **Next** to continue or **Cancel** to quit.

Step 2/5 - Select Report Type



Select Report Type

First, you must select the module the generated report is on: **Antivirus**, **Antispam**, **Content Filtering** and **Attachment Filtering**.

Then select one of the report types available for the module you have chosen.

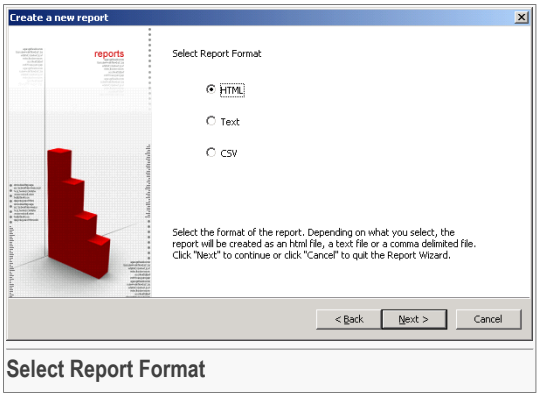
Note

For more information on the available report types, please refer to the table presented at the beginning of the "*Reports*" (p. 43) section.

Depending on your choice, the report may contain a summary of or only specific data about the activity of a specified component.

Click **Next**.

Step 3/5 - Select Report Format



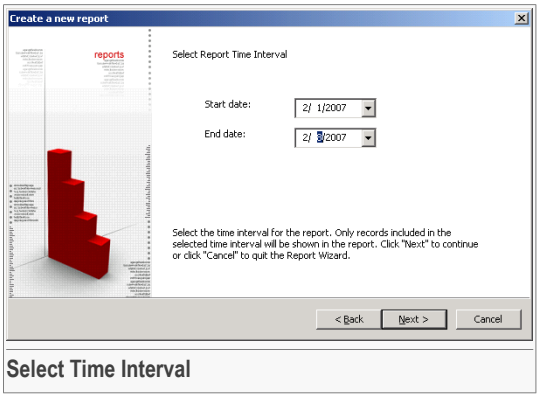
Select Report Format

Select the format of the report file (**HTML**, **text** or **CSV**).

Depending on your selection, the report will be created as an HTML, text or comma-separated values (CSV) file.

Click **Next**.

Step 4/5 - Select Time Interval



Select Time Interval

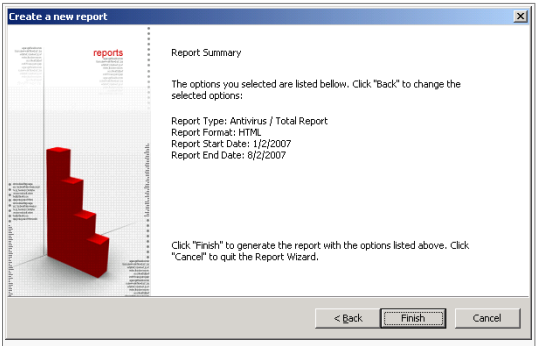
Select the time interval (**Start Date** and **End Date**) covered in the report. Only the records from the specified period will appear in the report.

To specify the start and end date, either click the numbers in the date field and enter new values or click **the arrow** to choose a date from the calendar.

Note
The date format is month/day/year.

Click **Next**.

Step 5/5 - View Summary



View Summary

This window allows you to view all of the report settings. You can change them by returning to the previous steps (click **Back**). If you do not want to make any changes, click **Finish**.

The report will appear in the Reports section.

8.2. Alerts & Logs

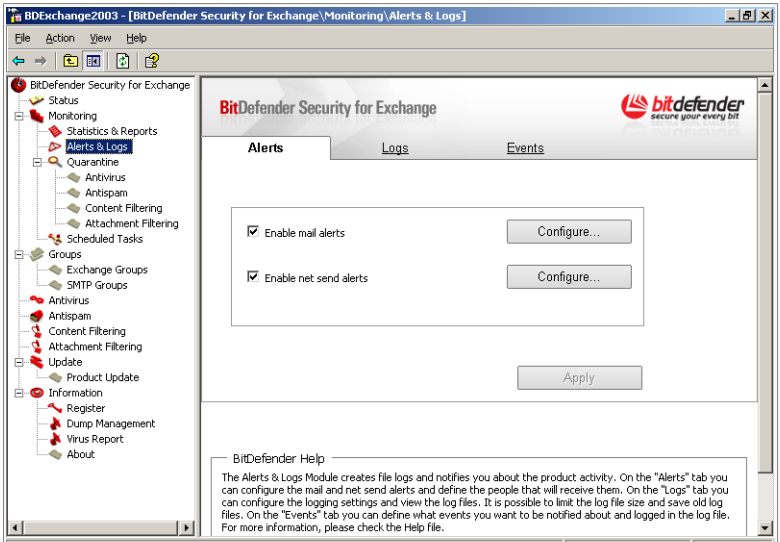
The **Alerts & Logs** module creates log files and notifies specified users of the occurrence of certain events regarding the product activity.

The module contains three sections:

- Alerts - allows you to enable the mail and net send alerts and to specify who will receive the alerts.
- Logs - allows you to enable and configure logging and to view the log files.
- Events - allows you to specify which events to keep a record of in the log file and, possibly, send alerts on to specified receivers.

8.2.1. Alerts

Click **Alerts & Logs** in the tree menu (**Monitoring** module) to enter this section.



Alerts

This is where you can enable the alert notification services and configure the global settings of the alerts.

Alerts are messages that include product-related information and which are meant to inform their receivers about the product activity. BitDefender can be set to notify users and administrators about occurring events through mail or net send alerts.

Mail Alerts

BitDefender can notify the network administrator by sending configurable mail alerts in case an event for which they have been set takes place. Enabling this alert will provide you with relevant and timely information about the status of your server, and may eliminate the need to access the BitDefender management console.

Note

This module integrates with an SMTP Server that does not require authentication. It works with an ESMTP server as well, but it does not use the ESMTP protocol because it is implemented on SMTP.

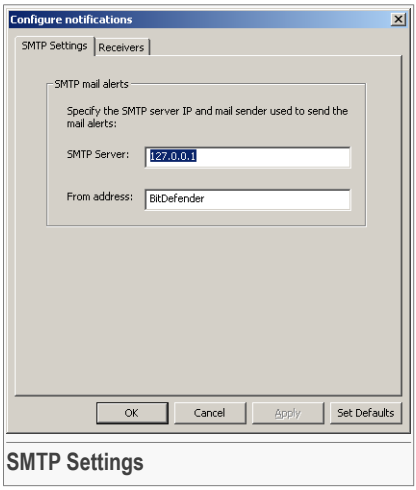
In order to use the mail notification service, follow these steps:

1. Check **Enable Mail Alerts** to activate the mail notification service and then click **Apply** to save the changes.
2. Configure the SMTP settings, as described in the "*Configuring Mail Alert Settings*" (p. 50) section.
3. Configure the receivers of the mail alerts, as described in the "*Configuring Mail Alert Receivers*" (p. 51) section.
4. Configure the events for which mail alerts should be sent, as described in the "*Configuring Events*" (p. 57) section.

If you want to disable this service, clear the check box corresponding to **Enable Mail Alerts** and then click **Apply** to save the changes.

Configuring Mail Alert Settings

To configure the SMTP settings of mail alerts click the corresponding **Configure** button. A new window will appear.



SMTP Settings

Specify the settings of the mail alerts:

- **SMTP Server** - type in the IP address of the SMTP server that your network uses to send messages.
- **From address** - type in the e-mail address that will appear in the sender field.

Important

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

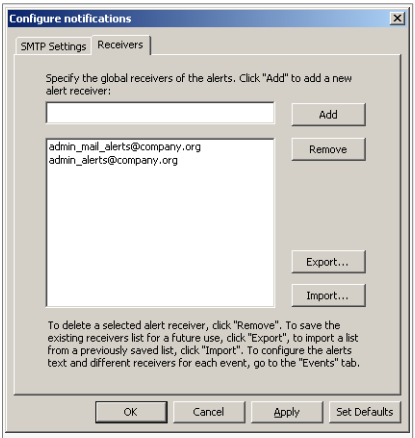
Click **Apply** to save the changes and **OK** to close the window.

Configuring Mail Alert Receivers

To configure the receivers of the mail alerts click the corresponding **Configure** button and then the **Receivers** tab. A new window will appear.

Note

The receivers specified here will be alerted upon the occurrence of an event for which this type of alert has been set. To specify different receivers for each event, go to the Events section and configure the events. For more information, please refer to "*Configuring Events*" (p. 57).



Receivers

Provide the e-mail address in the corresponding field and click **Add** to add the receiver to the list.

To import e-mail addresses from a `txt` file, click **Import**, select the file and then click **Open**.

If you want to export the list to a `txt` file, click **Export** and save the file to the desired location.

To remove one or several selected receivers click **Remove**.

Click **Apply** to save the changes and **OK** to close the window.

Net Send Alerts

BitDefender can notify the network administrator by sending configurable alerts through the `net send` command upon the occurrence of an event for which they have been set.

Note

This module integrates with the Net Send command of the Windows Operating System on which the product is installed and it provides alerts regarding the product activity. In order to receive such alerts, the Messenger and Alert services must be enabled by the administrator on the server and on the client workstations.

In order to use the net send notification service, follow these steps:

1. Check **Enable Net Send Alerts** to activate the net send notification service and then click **Apply** to save the changes.
2. Configure the receivers of the net send alerts, as described in the "*Configuring Net Send Alert Receivers*" (p. 53) section.
3. Configure the events for which net send alerts should be sent, as described in the "*Configuring Events*" (p. 57) section.

If you want to disable this service, clear the check box corresponding to **Enable Net Send Alerts** and then click **Apply** to save the changes.

Important

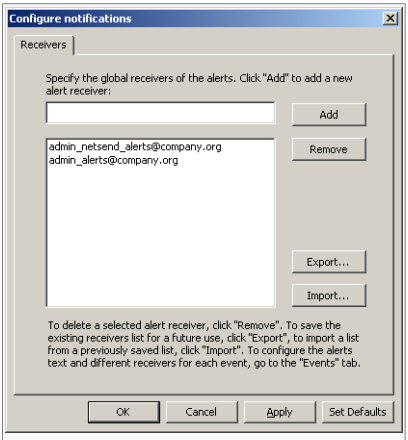
In case of a virus outbreak it is not advisable to use this type of alert.

Configuring Net Send Alert Receivers

To configure the receivers of the net send alerts click the corresponding **Configure** button. A new window will appear.

Note

The receivers specified here will be alerted upon the occurrence of an event for which this type of alert has been set. To specify different receivers for each event, go to the Events section and configure the events. For more information, please refer to "*Configuring Events*" (p. 57).



Receivers

Provide the computer name in the corresponding field and click **Add** to add the receiver to the list.

To import computer names from a `txt` file, click **Import**, select the file and then click **Open**.

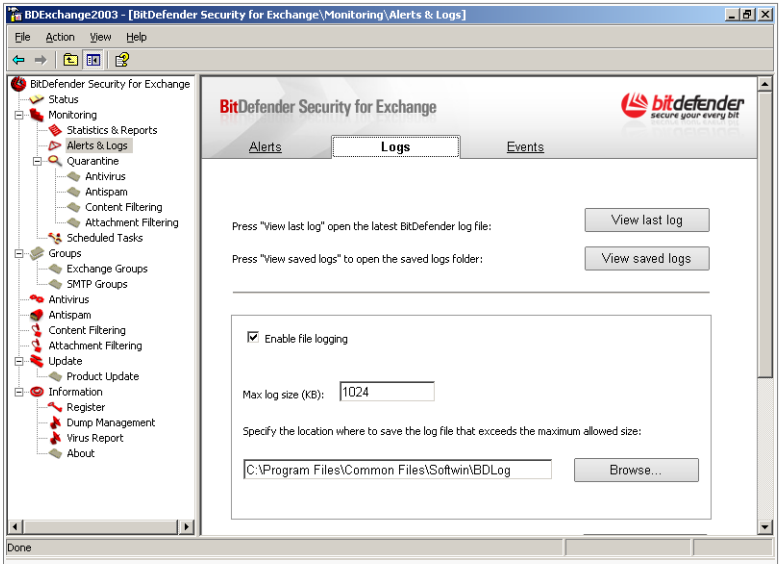
If you want to export the list to a `txt` file, click **Export** and save the file to the desired location.

To remove one or several selected receivers click **Remove**.

Click **Apply** to save the changes and **OK** to close the window.

8.2.2. Logs

Click **Alerts & Logs** in the tree menu (**Monitoring** module) and then the **Logs** tab to enter this section.



Logs

This is where you can enable logging and view the log files.

BitDefender can be set to keep a log of its activity. The log file contains a record of all of the enabled events that took place while the logging option was enabled.

Note

By default, the log file is saved in: `C:\Program Files\Common Files\Softwin\BDLog`.

Configuring Logging

To log the product activity to a file, check **Enable file logging**.

BitDefender creates the log file in `C:\Program Files\Common Files\Softwin\BDLog`. By default, when the file reaches the size limit of 1024 KB, a new log file is created.

Specify the size limit of the log files in the **Maximum log file size** field. If you do not want to limit the size of the log file, enter 0 in the edit field.

You can specify a folder where files exceeding the specified size limit should be saved. Either provide its path in the corresponding field or click **Browse**, locate the folder and then click **OK** to set the location.

Click **Apply** to save the changes.

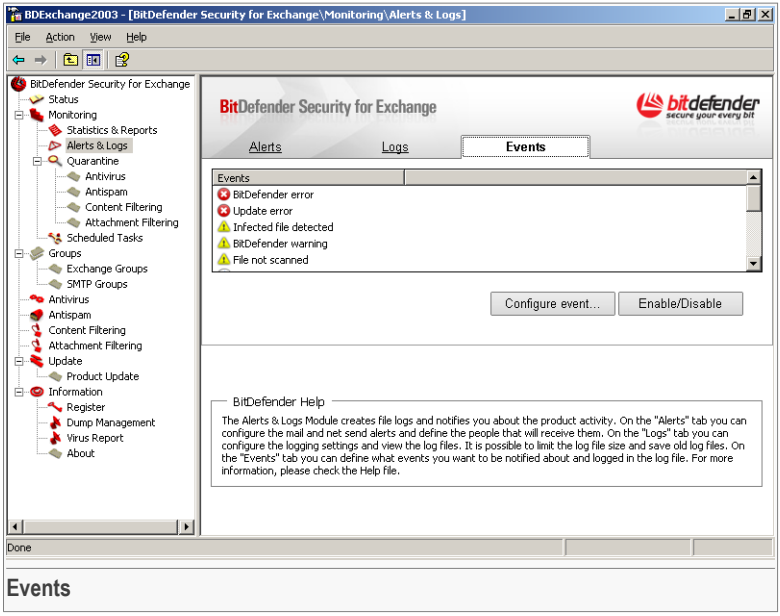
Examining Logs

Click **View last log** to open the last log file.

If you have set a size limit for the log file, you can see any saved log file. Click **View saved logs**, locate the log file you want to see and double-click it.

8.2.3. Events

Click **Alerts & Logs** in the tree menu (**Monitoring** module) and then the **Events** tab to enter this section.



Events

This is where you can manage and configure the events. You can choose to log an event and to alert specific receivers about its occurrence.

There are 3 types of events:

- **Information** - provide information about the product activity.
- **Warning** - provide critical information about aspects of the product activity which require your attention.
- **Error** - provide information about errors that appear during product operation.

Here is a list of the events that may appear:

Event	Description
BitDefender Error	Groups all the errors that may appear during product operation, such as service start failure.
Update Error	Refers to the occurrence of an error during the update process.
Infected file detected	Occurs when an infected file has been detected.
BitDefender Warning	Groups critical information regarding the activity of BitDefender.
File not scanned	Occurs when a file could not be scanned by BitDefender.
BitDefender information	Groups information regarding the activity of BitDefender.
Key expired	Indicates the expiration of the registration period.
Key will expire	Indicates that there are 3 days left before the product expires.
On-demand scanning	Occurs whenever an on-demand scan is performed.
Rule matched	Occurs whenever a message matches a Content Filtering or Attachment Filtering rule.
Update information	Contains information about the update process.
Product update	Occurs when a product update is available.
Report generated	Occurs whenever a report is generated.

Managing Events

All of the events that may occur occurred are listed in a table.

To manage the events, use the following buttons:

- **Configure event** - opens the configuration window of a selected event, allowing you to configure the importance level of the event and, if necessary, the mail and net send alerts issued when the event occurs. For more information, please refer to "*Configuring Events*" (p. 57).
- **Enable / Disable** - enables / disables one or several selected events.

Note

If an event is disabled, it will not be recorded and no alert will be sent when it takes place.

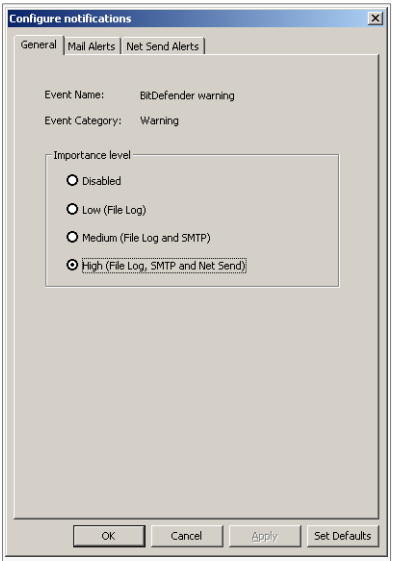
Configuring Events

To configure an event, select it and click **Configure event**. The configuration window will appear.

Follow these steps to configure an event:

Step 1/3 - Select Event Importance

Open the configuration window to select the importance of the event.



Select Event Importance

You can see the name and category of the event.

When an event takes place, based on its importance, it can be logged and, possibly, specified receivers may be notified through mail and net send alerts of its occurrence. Choose one of the following options to set the importance level:

- **Disabled** - to disable the event. This means that no record of the event will be kept and no alert will be sent when the event takes place.
- **Low (File Log)** - to keep a record of the event in the log file. No alert will be sent when the event takes place.
- **Medium (File Log and SMTP)** - to log the event and send mail alerts when the event takes place.
- **High (File Log, SMTP and Net Send)** - to log the event and send mail and net send alerts when the event takes place.

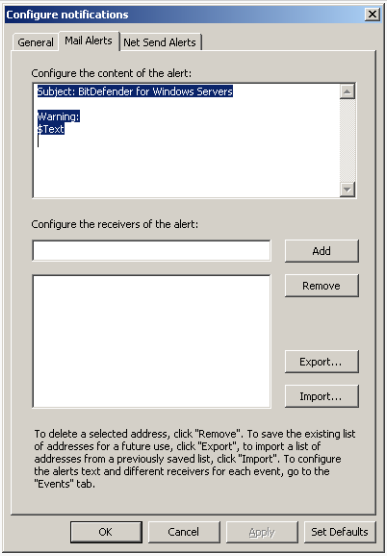
Note

To make sure that file logging and mail and net send notification services are enabled, go to the Logs and Alerts sections.

Click **Apply** to save the changes and **OK** if you want to close the window.

Step 2/3 - Configure Mail Alerts

If the importance of the event is medium or high, mail alerts will be sent. Click the **Mail Alerts** tab to configure the mail alerts.



Configure Mail Alerts

Configure Alert Text

BitDefender allows you to configure the alert content. You can see the default text in the box.

Make the desired changes to the alert content.

Important

We recommend you NOT to modify the strings that begin with the $ symbol as they provide valuable information about the event.

Configure Alert Receivers

Provide the e-mail address in the corresponding field and click **Add** to add the receiver to the list.

Note

Beside the receivers defined here, the alert will also be sent to those defined in the Alerts section (see "*Configuring Mail Alert Receivers*" (p. 51)).

To import e-mail addresses from a `txt` file, click **Import**, select the file and then click **Open**.

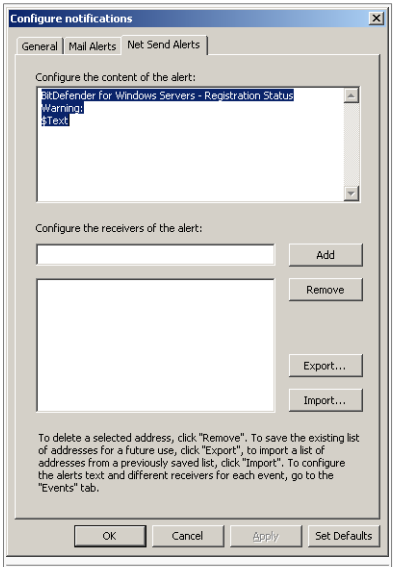
If you want to export the list to a `txt` file, click **Export** and save the file to the desired location.

To remove one or several selected receivers click **Remove**.

Click **Apply** to save the changes and **OK** if you want to close the window.

Step 3/3 - Configure Net Send Alerts

If the importance of the event is high, net send alerts will be sent. Click the **Net Send Alerts** tab to configure the net send alerts.



Configure Net Send Alerts

Configure Alert Text

BitDefender allows you to configure the alert content. You can see the default text in the box.

Make the desired changes to the alert content.

Important

We recommend you NOT to modify the strings that begin with the `$` symbol as they provide valuable information about the event.

Configure Alert Receivers

Provide the computer name in the corresponding field and click **Add** to add the receiver to the list.

Note

Beside the receivers defined here, the alert will also be sent to those defined in the Alerts section (see "*Configuring Net Send Alert Receivers*" (p. 53)).

To import computer names from a `txt` file, click **Import**, select the file and then click **Open**.

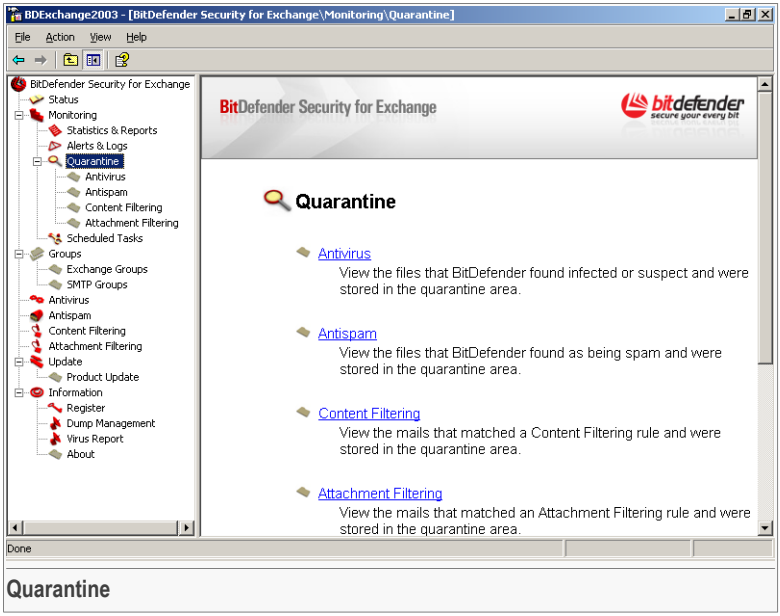
If you want to export the list to a `txt` file, click **Export** and save the file to the desired location.

To remove one or several selected receivers click **Remove**.

Click **Apply** to save the changes and **OK** to close the window.

8.3. Quarantine

Click **Quarantine** in the tree menu (**Monitoring** module) to enter this section.



Quarantine

This is where you can find all of the quarantined files.

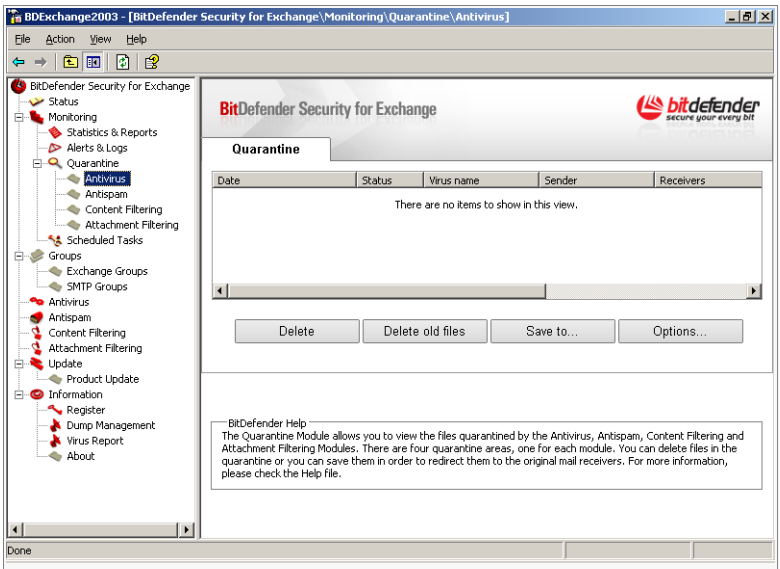
The **Quarantine** is divided into 4 areas:

- Antivirus - contains the objects that BitDefender found infected or suspect and which were stored in the quarantine area.
- Antispam - contains the messages that BitDefender found as being spam and which were stored in the quarantine area.
- Content Filtering - contains the messages that matched a Content Filtering rule and which were stored in the quarantine area.
- Attachment Filtering - contains the messages that matched an Attachment Filtering and which were stored in the quarantine area.

Click a link to see the quarantined files for the corresponding component.

8.3.1. Antivirus Quarantine

Click **Antivirus** in the tree menu (**Quarantine** module) to enter this section.



Antivirus Quarantine

This is where you can see the objects that BitDefender found infected or suspect and which were stored in the quarantine area.

There are two types of quarantined objects: mail body and mail attachment. For each file, the following information is provided: the date and time when it was quarantined, the status (infected / suspect / unscanable), the virus name, the mail address or mailbox of the sender, the mail address or mailbox of the receivers, the subject of the message and the file name (for attachments).

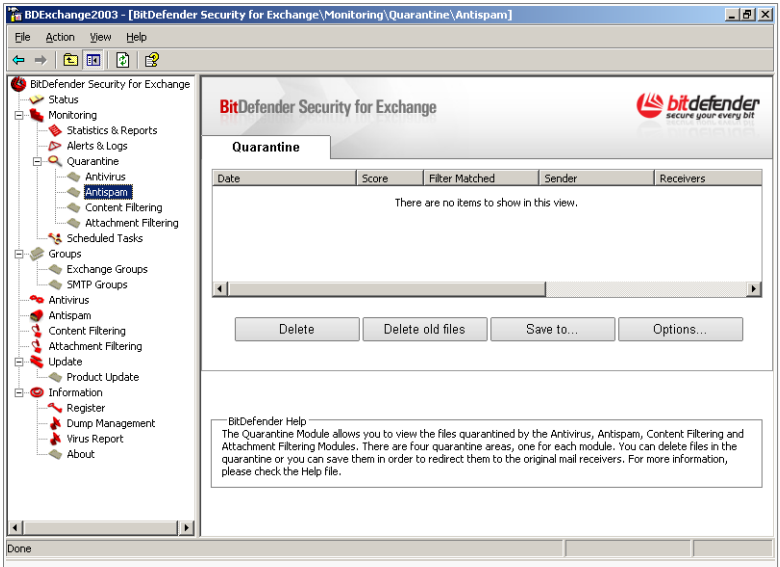
Quarantined files are encrypted. In order to see an item from the quarantine area, select it and then click **Save to disk** to decrypt the file. This way you can analyze the item and send it by mail.

Note

To learn how to manage the quarantined files and the quarantine area, please refer to "*Managing Quarantine*" (p. 67).

8.3.2. Antispam Quarantine

Click **Antispam** in the tree menu (**Quarantine** module) to enter this section.



Antispam Quarantine

This is where you can see the messages that BitDefender found as being spam and which were stored in the quarantine area.

For each quarantined file, the following information is provided: the date and time when it was quarantined, the spam score received, the virus name, the mail address of the sender, the mail address of the receivers, the subject and the file name of the message.

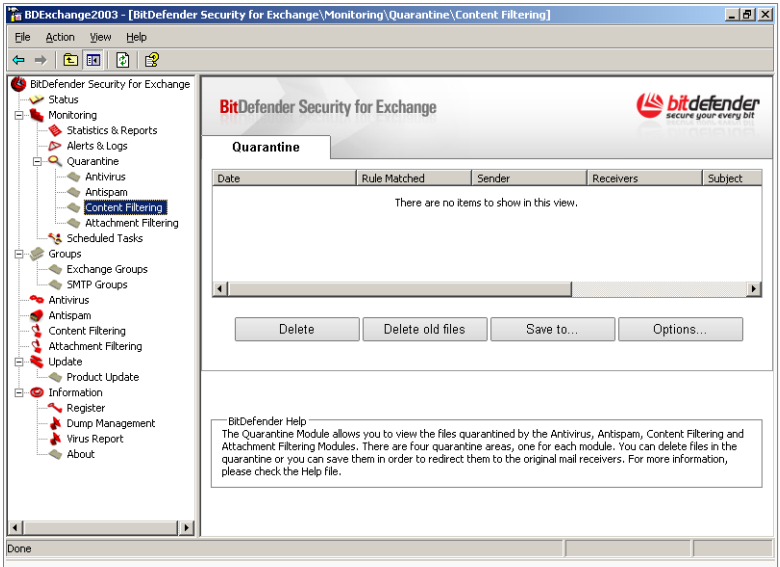
Quarantined files are encrypted. In order to see an item from the quarantine area, select it and then click **Save to disk** to decrypt the file. This way you can analyze the item and send it by mail.

Note

To learn how to manage the quarantined files and the quarantine area, please refer to "*Managing Quarantine*" (p. 67).

8.3.3. Content Filtering Quarantine

Click **Content Filtering** in the tree menu (**Quarantine** module) to enter this section.



Content Filtering Quarantine

This is where you can see the messages that matched a Content Filtering rule and which were stored in the quarantine area.

For each quarantined file, the following information is provided: the date and time when it was quarantined, the matching rule, the mail address of the sender, the mail address of the receivers, the subject and the file name of the message.

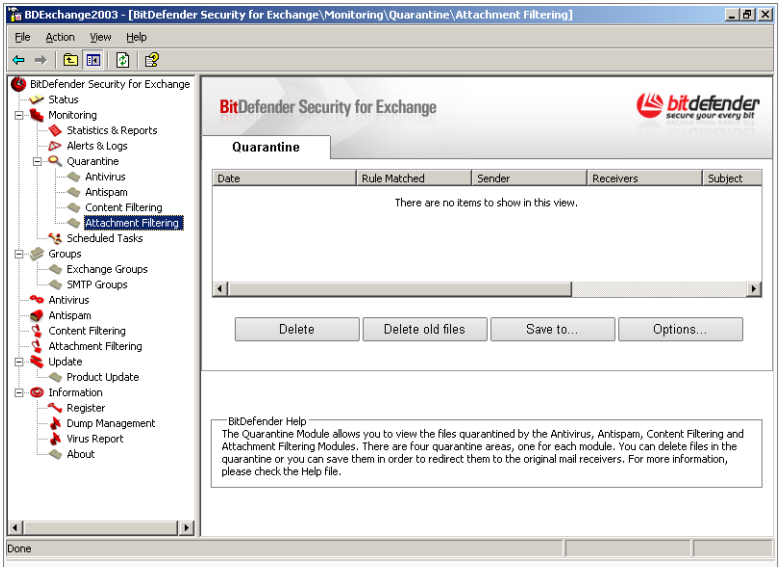
Quarantined files are encrypted. In order to see an item from the quarantine area, select it and then click **Save to disk** to decrypt the file. This way you can analyze the item and send it by mail.

Note

To learn how to manage the quarantined files and the quarantine area, please refer to “*Managing Quarantine*” (p. 67).

8.3.4. Attachment Filtering Quarantine

Click **Attachment Filtering** in the tree menu (**Quarantine** module) to enter this section.



Attachment Filtering Quarantine

This is where you can see the messages that matched an Attachment Filtering rule and which were stored in the quarantine area.

For each quarantined file, the following information is provided: the date and time when it was quarantined, the matching rule, the mail address of the sender, the mail address of the receivers, the subject and the file name of the message.

Quarantined files are encrypted. In order to see an item from the quarantine area, select it and then click **Save to disk** to decrypt the file. This way you can analyze the item and send it by mail.

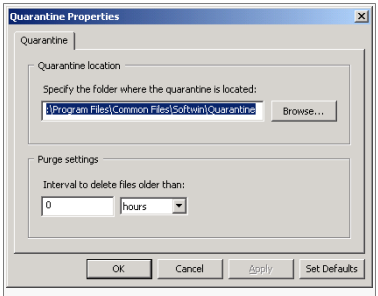
Note

To learn how to manage the quarantined files and the quarantine area, please refer to "*Managing Quarantine*" (p. 67).

8.3.5. Managing Quarantine

To manage the quarantined files and the quarantine areas, use the following buttons:

- **Delete** - deletes one or several selected files.
- **Delete old files** - deletes the files older than a specified time interval. Click **Properties** to specify this interval.
- **Save to** - decrypts the quarantined files and saves them to the disk. This way you can see and analyze the quarantined item (message / attachment).
- **Properties** - opens a window where you can specify the quarantine settings.



Quarantine

You can change the folder the quarantine is located in. Provide the new path in the edit field or click **Browse** to set a new location. The default location of the quarantine folders is: `C:\Program Files\Common Files\Softwin\Quarantine`.

Note

The default quarantine folders for each component are the following:

- `C:\Program Files\Common Files\Softwin\Quarantine\AV` for the Antivirus module.
- `C:\Program Files\Common Files\Softwin\Quarantine\AS` for the Antispam module.
- `C:\Program Files\Common Files\Softwin\Quarantine\CF` for the Content Filtering module.
- `C:\Program Files\Common Files\Softwin\Quarantine\AF` for the Attachment Filtering module.

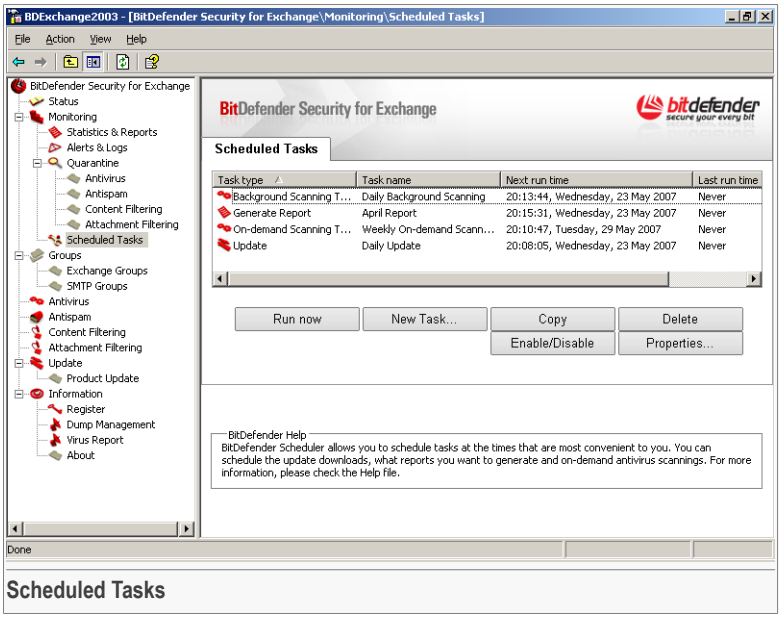
If you want to delete quarantined files older than a specified time interval, provide the number of hours / days / weeks / months in the corresponding field. The default

interval is 90 days. You must click **Delete old files** periodically in order to delete files older than the specified period.

Click **OK** to save the changes and close the window. If you want to apply the default settings, click **Set Defaults**.

8.4. Scheduled Tasks

Click **Scheduled Tasks** in the tree menu (**Monitoring** module) to enter this section.



Scheduled Tasks

This is where you can schedule:

- on-demand scanning processes.
- background scanning processes.
- update processes.
- report generation tasks.

Here you can also manage and view the existing scheduled tasks.

8.4.1. Managing Scheduled Tasks

You can see all the existing scheduled tasks listed in the table. For each task, the following information is provided: the task type and name, the last time when it was performed, the next time it is scheduled to run and the status.

To manage the scheduled tasks, use these buttons:

- **Run Now** - runs a selected scheduled task.
- **New Task** - launches a wizard that will help you create a new scheduled task.

Note

The configuration wizard is different for each type of scheduled task.

- **Copy** - copies one or several selected scheduled tasks.
- **Delete** - deletes one or several selected scheduled tasks. You will have to confirm your choice by clicking **Yes**.
- **Enable / Disable** - enables / disables one or several selected scheduled tasks.
- **Properties** - opens the configuration window of a selected scheduled task, allowing you to modify it and to configure more advanced settings.

8.4.2. Update Tasks

Scheduling Tasks

To create a new scheduled task, click **New task**. The configuration wizard will appear. It will guide you through the process of creating a scheduled task.

Note

The scheduled update tasks will not deactivate the automatic update.

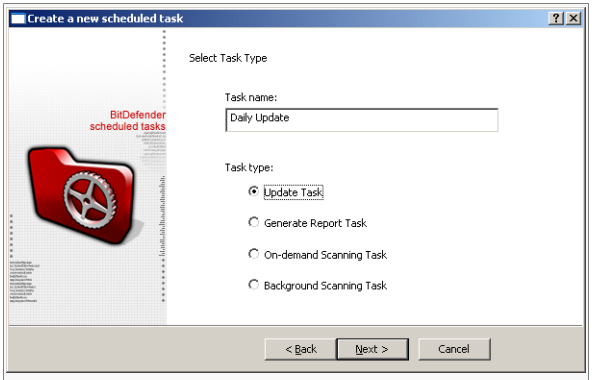
Follow these steps to schedule an update task:

Step 1/4 - Welcome to the Scheduled Tasks Wizard

Welcome

Click **Next**.

Step 2/4 - Select Task Type

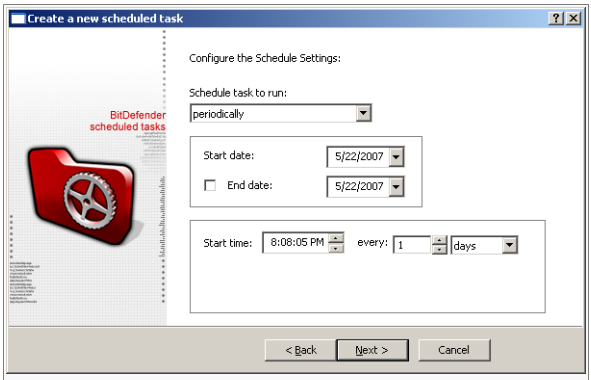


Select Task Type

Provide the task name and then select **Update Task**.

Click **Next**.

Step 3/4 - Configure Schedule



Run Task Periodically

Specify the task schedule.

You must choose one of the following options from the menu:

- **Once** - to run the task one time only, at a given moment.

  Specify the start date and time in the **Start Date / Start Time** fields.

- **Periodically** - to run the task periodically, at certain time intervals (minutes, hours, days, weeks, months, years), starting with a specified date and time.

  To configure the necessary settings, follow these steps:

  1. Specify the start date in the **Start Date** field.
  2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in the corresponding field.
  3. Specify the start time in the **Start Time** field.
  4. Specify the task frequency by specifying the number of minutes / hours / days / weeks / months / years between two successive occurrences of such task, in the corresponding field..

- **Week Days** - to run the task repeatedly only in certain days of the week starting with a specified date and time.

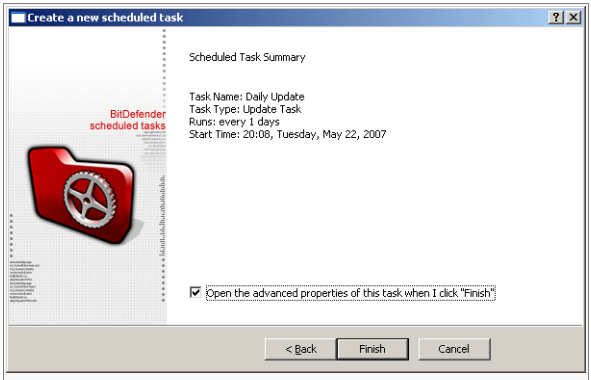
  To configure the necessary settings, follow these steps:

  1. Specify the start date in the **Start Date** field.

2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in corresponding field.
3. Specify the start time in the **Start Time** field.
4. Specify the day or days of the week on which the task should be run.

Click **Next**.

Step 4/4 - View Summary



View Summary

This window allows you to view the task settings and make any changes by returning to the previous steps (**Back**). If you do not want to make any changes, click **Finish**.

Check **Open the advanced properties of this task when I click "Finish"** if you want the **Properties** window of this task to be opened after you complete the wizard. In this window you can modify the task and configure more advanced settings. For more information, please refer to "*Configuring Properties*" (p. 72).

Note

The task will appear in the Scheduled Tasks section.

Configuring Properties

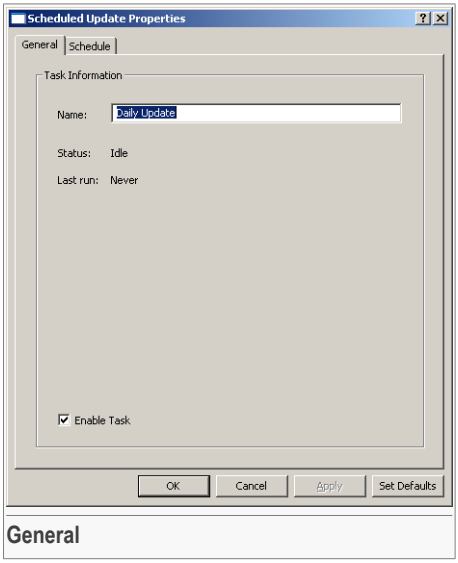
In order to modify an existing scheduled task or to configure more advanced settings, unavailable in the configuration wizard, just double-click the task or select it and click **Properties**. The configuration window will appear.

Note

To open the configuration window, you can also check **Open the advanced properties of this task when I click "Finish"** in the last step of the wizard.

Viewing General Information

Open the configuration window to check general information.



General

You can see general information about the task (the name, the status, the last time when the task ran). If you want to change the task name, enter a new name in the corresponding field.

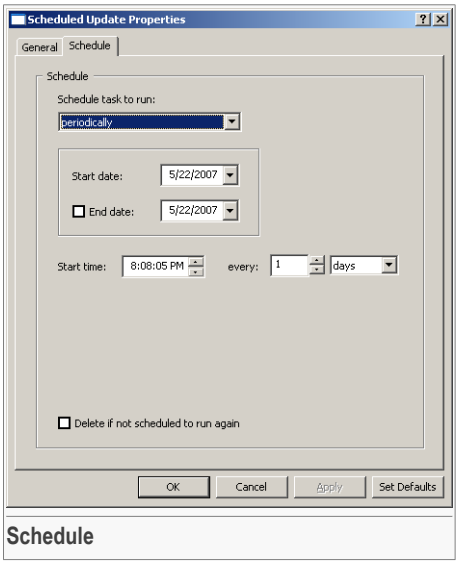
To enable the task, check **Enable Task**. If you want to disable the task, clear the check box.

Click **Apply** to the save changes. If you want to save the changes and close the configuration window, click **OK**.

If you want to close the configuration window without making any changes, click **Cancel**.

Modifying Schedule

Click the **Schedule** tab in the configuration window to modify the schedule.



Schedule

Specify the task schedule.

You must choose one of the following options from the menu:

- **Once** - to run the task one time only, at a given moment.

  Specify the start date and time in the **Start Date / Start Time** fields.

- **Periodically** - to run the task periodically, at certain time intervals (minutes, hours, days, weeks, months, years), starting with a specified date and time.

  To configure the necessary settings, follow these steps:

  1. Specify the start date in the **Start Date** field.
  2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in the corresponding field.
  3. Specify the start time in the **Start Time** field.
  4. Specify the task frequency by specifying the number of minutes / hours / days / weeks / months / years between two successive occurrences of such task, in the corresponding field..

- **Week Days** - to run the task repeatedly only in certain days of the week starting with a specified date and time.

To configure the necessary settings, follow these steps:

1. Specify the start date in the **Start Date** field.
2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in corresponding field.
3. Specify the start time in the **Start Time** field.
4. Specify the day or days of the week on which the task should be run.

Check **Delete if not scheduled to run again** to delete the task after its last execution.

Click **Apply** to the save changes. If you want to save the changes and close the configuration window, click **OK**.

If you want to close the configuration window without making any changes, click **Cancel**.

8.4.3. Report Generation Tasks

Scheduling Tasks

To create a new scheduled task, click **New task**. The configuration wizard will appear. It will guide you through the process of creating a scheduled task.

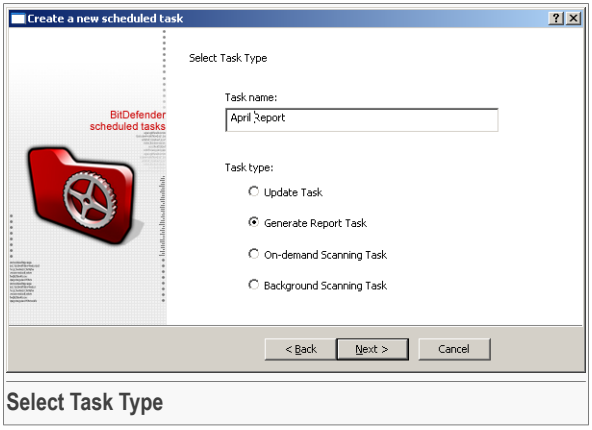
Follow these steps to schedule a report generation task:

Step 1/7 - Welcome to the Scheduled Tasks Wizard

Welcome

Click **Next**.

Step 2/7 - Select Task Type

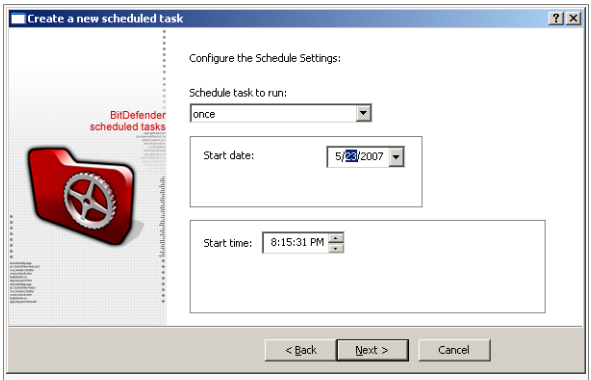


Select Task Type

Provide the task name and then select **Generate Report Task**.

Click **Next**.

Step 3/7 - Configure Schedule



Run Task Periodically

Specify the task schedule.

You must choose one of the following options from the menu:

- **Once** - to run the task one time only, at a given moment.

  Specify the start date and time in the **Start Date / Start Time** fields.

- **Periodically** - to run the task periodically, at certain time intervals (minutes, hours, days, weeks, months, years), starting with a specified date and time.

  To configure the necessary settings, follow these steps:

  1. Specify the start date in the **Start Date** field.
  2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in the corresponding field.
  3. Specify the start time in the **Start Time** field.
  4. Specify the task frequency by specifying the number of minutes / hours / days / weeks / months / years between two successive occurrences of such task, in the corresponding field..

- **Week Days** - to run the task repeatedly only in certain days of the week starting with a specified date and time.

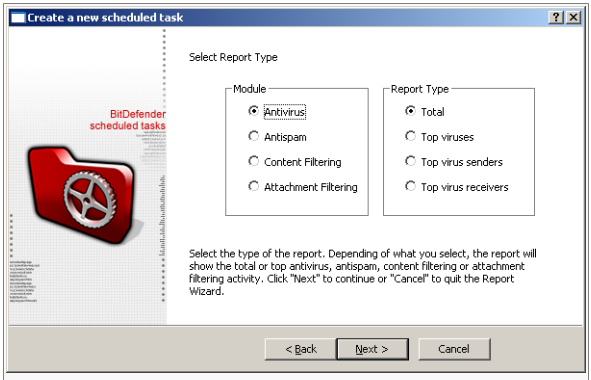
  To configure the necessary settings, follow these steps:

  1. Specify the start date in the **Start Date** field.

2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in corresponding field.
3. Specify the start time in the **Start Time** field.
4. Specify the day or days of the week on which the task should be run.

Click **Next**.

Step 4/7 - Select Report Type



Select Report Type

First, you must select the module the generated report is on: **Antivirus**, **Antispam**, **Content Filtering** and **Attachment Filtering**.

Then select one of the report types available for the module you have chosen.

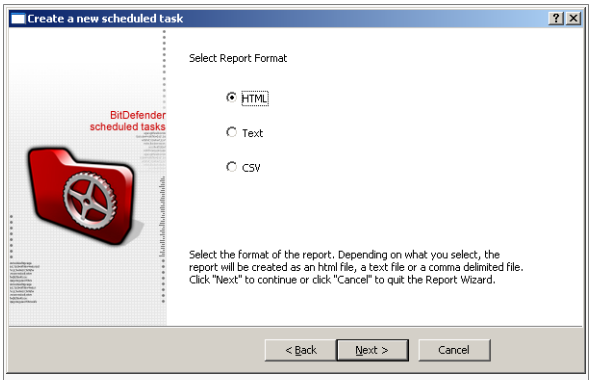
Note

For more information on the available report types, please refer to the table presented at the beginning of the "*Reports*" (p. 43) section.

Depending on your choice, the report may contain a summary of or only specific data about the activity of a specified component.

Click **Next**.

Step 5/7 - Select Report Format



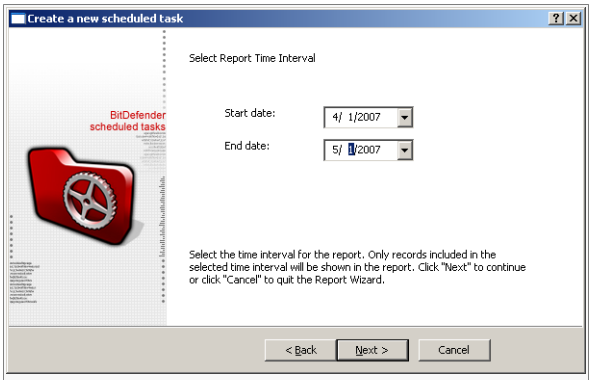
Select Report Format

Select the format of the report file (**HTML**, **text** or **CSV**).

Depending on your selection, the report will be created as an HTML, text or comma-separated values (CSV) file.

Click **Next**.

Step 6/7 - Select Time Interval



Select Time Interval

Select the time interval (**Start Date** and **End Date**) covered in the report. Only the records from the specified period will appear in the report.

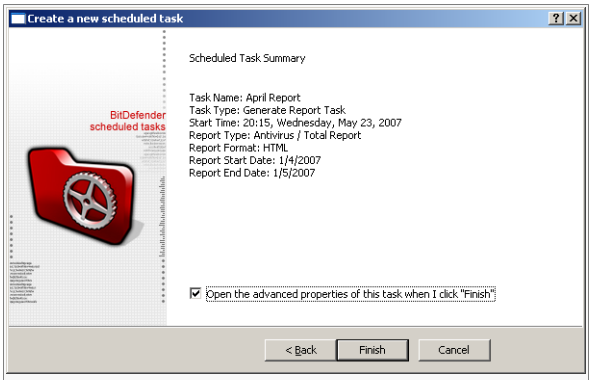
To specify the start and end date, either click the numbers in the date field and enter new values or click **the arrow** to choose a date from the calendar.

Note

The date format is month/day/year.

Click **Next**.

Step 7/7 - View Summary



View Summary

This window allows you to view the task settings and make any changes by returning to the previous steps (**Back**). If you do not want to make any changes, click **Finish**.

Check **Open the advanced properties of this task when I click "Finish"** if you want the **Properties** window of this task to be opened after you complete the wizard. In this window you can modify the task and configure more advanced settings. For more information, please refer to "*Configuring Properties*" (p. 81).

Note

The task will appear in the Scheduled Tasks section.

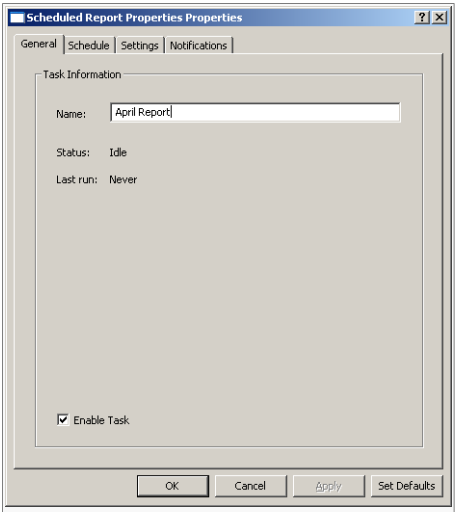
Configuring Properties

In order to modify an existing scheduled task or to configure more advanced settings, unavailable in the configuration wizard, just double-click the task or select it and click **Properties**. The configuration window will appear.

Note

To open the configuration window, you can also check **Open the advanced properties of this task when I click "Finish"** in the last step of the wizard.

Viewing General Information



General

You can see general information about the task (the name, the status, the last time when the task ran). If you want to change the task name, enter a new name in the corresponding field.

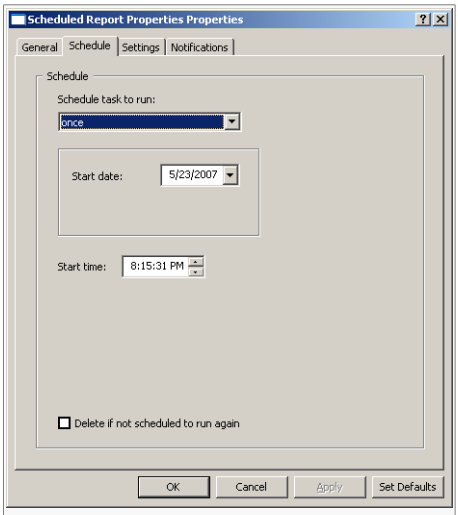
To enable the task, check **Enable Task**. If you want to disable the task, clear the check box.

Click **Apply** to the save changes. If you want to save the changes and close the configuration window, click **OK**.

If you want to close the configuration window without making any changes, click **Cancel**.

Modifying Schedule

Click the **Schedule** tab in the configuration window to modify the schedule.



Schedule

Specify the task schedule.

You must choose one of the following options from the menu:

- **Once** - to run the task one time only, at a given moment.

  Specify the start date and time in the **Start Date / Start Time** fields.

- **Periodically** - to run the task periodically, at certain time intervals (minutes, hours, days, weeks, months, years), starting with a specified date and time.

  To configure the necessary settings, follow these steps:

  1. Specify the start date in the **Start Date** field.
  2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in the corresponding field.
  3. Specify the start time in the **Start Time** field.
  4. Specify the task frequency by specifying the number of minutes / hours / days / weeks / months / years between two successive occurrences of such task, in the corresponding field..

- **Week Days** - to run the task repeatedly only in certain days of the week starting with a specified date and time.

To configure the necessary settings, follow these steps:

1. Specify the start date in the **Start Date** field.
2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in corresponding field.
3. Specify the start time in the **Start Time** field.
4. Specify the day or days of the week on which the task should be run.

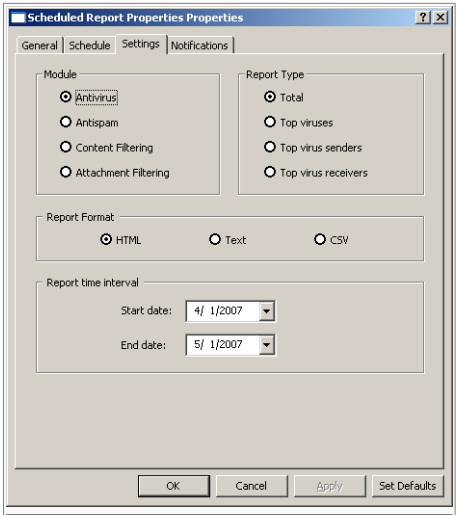
Check **Delete if not scheduled to run again** to delete the task after its last execution.

Click **Apply** to the save changes. If you want to save the changes and close the configuration window, click **OK**.

If you want to close the configuration window without making any changes, click **Cancel**.

Configuring Settings

Click the **Settings** tab in the configuration window to modify the report settings.



Settings

Follow these steps to configure the report settings:

1. Choose on which module (Antivirus, Antispam, Content Filtering, Attachment Filtering) to generate the report.
2. Select one of the report types available for the previously specified module.

Note

For more information on the available report types, please refer to the table presented at the beginning of the "*Reports*" (p. 43) section.

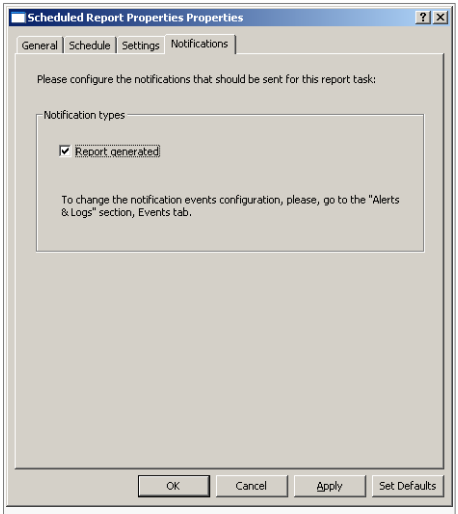
3. Select the format of the report file (**HTML**, **text** or **CSV**).
4. Select the time interval (**Start Date** and **End Date**) covered in the report.

Click **Apply** to the save changes. If you want to save the changes and close the configuration window, click **OK**.

If you want to close the configuration window without making any changes, click **Cancel**.

Configuring Notifications

Click the **Notifications** tab in the configuration window to configure notifications.



Notifications

Check **Report Generated** to enable notifications on report generation.

Note

To choose how to obtain information about the occurrence of this event, go to the **Alerts&Events** module, Events section and configure the corresponding event.

Click **Apply** to the save changes. If you want to save the changes and close the configuration window, click **OK**.

If you want to close the configuration window without making any changes, click **Cancel**.

8.4.4. On-demand Scanning Tasks

Scheduling Tasks

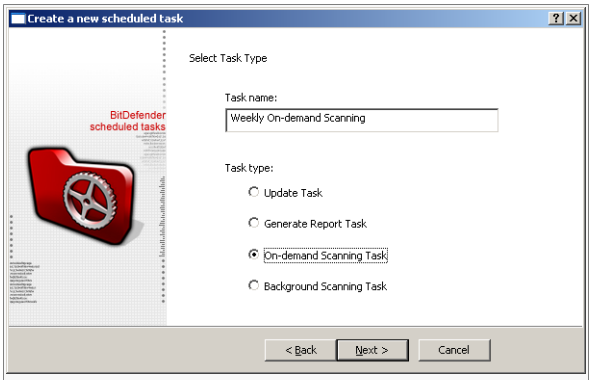
To create a new scheduled task, click **New task**. The configuration wizard will appear. It will guide you through the process of creating a scheduled task.

Follow these steps to schedule an on-demand scanning task:

Step 1/7 - Welcome to the Scheduled Tasks Wizard

Click **Next**.

Step 2/7 - Select Task Type

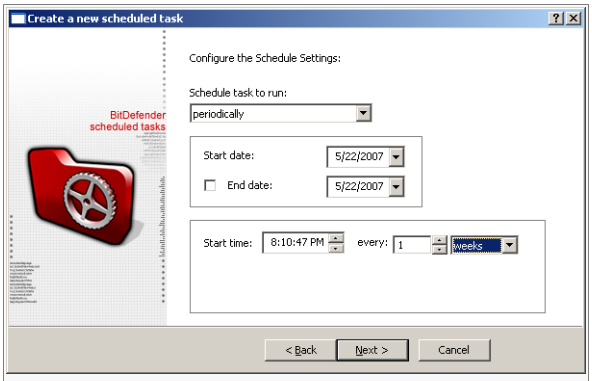


Select Task Type

Provide the task name and then select **On-demand Scanning Task**.

Click **Next**.

Step 3/7 - Configure Schedule



Run Task Periodically

Specify the task schedule.

You must choose one of the following options from the menu:

- **Once** - to run the task one time only, at a given moment.

  Specify the start date and time in the **Start Date / Start Time** fields.

- **Periodically** - to run the task periodically, at certain time intervals (minutes, hours, days, weeks, months, years), starting with a specified date and time.

  To configure the necessary settings, follow these steps:

  1. Specify the start date in the **Start Date** field.
  2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in the corresponding field.
  3. Specify the start time in the **Start Time** field.
  4. Specify the task frequency by specifying the number of minutes / hours / days / weeks / months / years between two successive occurrences of such task, in the corresponding field..

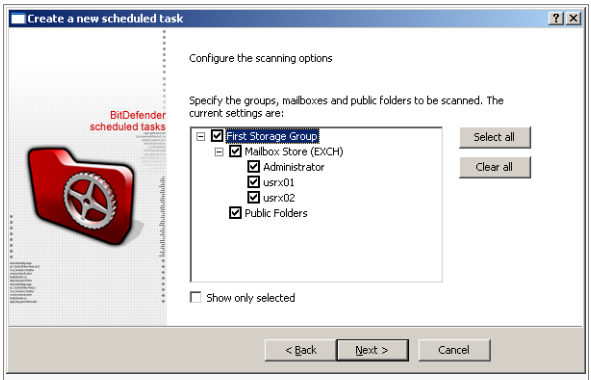
- **Week Days** - to run the task repeatedly only in certain days of the week starting with a specified date and time.

  To configure the necessary settings, follow these steps:

  1. Specify the start date in the **Start Date** field.
  2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in corresponding field.
  3. Specify the start time in the **Start Time** field.
  4. Specify the day or days of the week on which the task should be run.

Click **Next**.

Step 4/7 - Select Scan Target



Select Scan Target

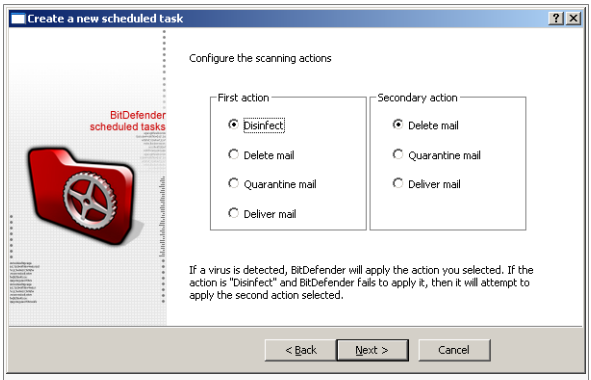
Check the items (groups, mailboxes and public folders) you want to be scanned.

Click **Select All** to check all items. If you click **Clear All** no item will be selected.

If you want to see only the selected items, check **Show only selected**.

Click **Next**.

Step 5/7 - Set Action



Set Action

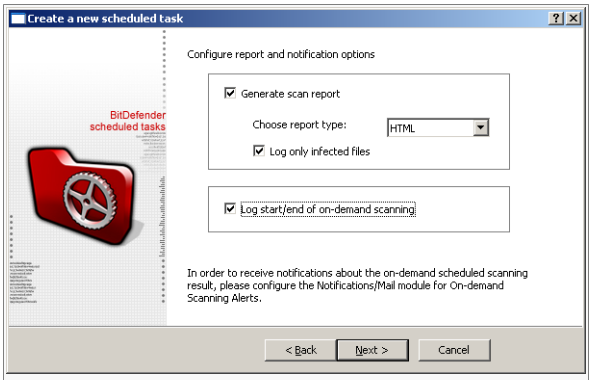
Set the action to be taken on the infected messages.

You must choose one of the following actions:

Action	Description
Disinfect	The infected messages are disinfected. You can choose a second action to be taken on the infected messages if disinfection fails. The second action options are delete, quarantine, deliver mail (as defined below).
Delete mail	The infected messages are deleted.
Quarantine mail	The infected messages are moved to the quarantine folder.
Deliver mail	The infected messages are delivered in full to their receivers.

Click **Next**.

Step 6/7 - Configure Notifications Options



Configure Notifications Options

Configure Report Options

Check **Generate Scan Report** to generate a report for the on-demand scan. The default location of the report file is: `C:\Program Files\Softwin\BitDefender Security for Exchange\Reports`.

You can choose the format of the report file from the menu. The report can be generated in HTML, text or CSV format.

If you want only the infected / suspect files to be logged in the report, check the corresponding option.

Note

To view the report file, at the end of the scanning, open the configuration window (select the task and click **Properties**) and then click **View Log**.

Log Scanning

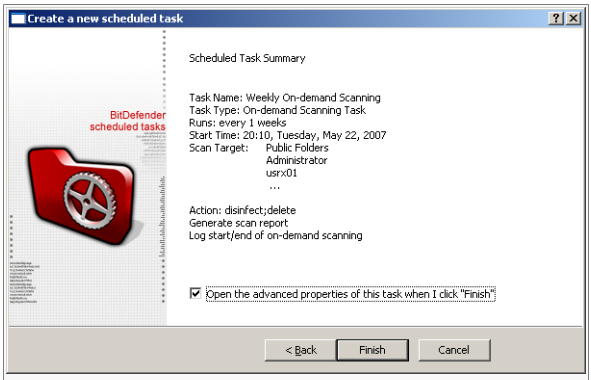
Check **Log start/end of on-demand scanning** to record the start and the end of the process in the log file.

Note

The corresponding event from the Events section must be enabled and properly configured. For more information, please refer to "*Configuring Events*" (p. 57).

Click **Next**.

Step 7/7 - View Summary



View Summary

This window allows you to view the task settings and make any changes by returning to the previous steps (**Back**). If you do not want to make any changes, click **Finish**.

Check **Open the advanced properties of this task when I click "Finish"** if you want the **Properties** window of this task to be opened after you complete the wizard. In this window you can modify the task and configure more advanced settings. For more information, please refer to "*Configuring Properties*" (p. 92).

Note

The task will appear in the Scheduled Tasks section.

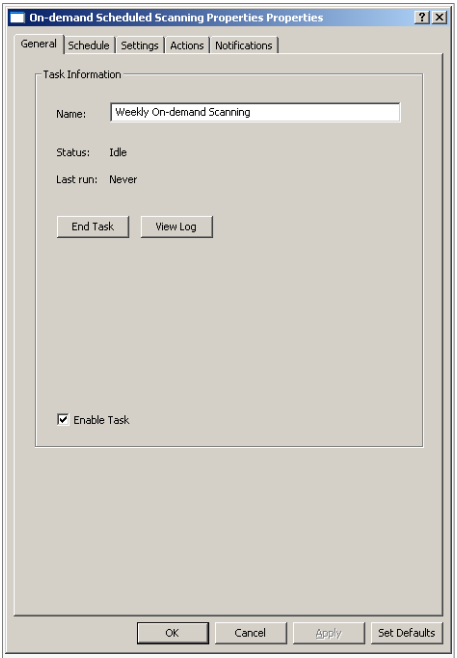
Configuring Properties

In order to modify an existing scheduled task or to configure more advanced settings, unavailable in the configuration wizard, just double-click the task or select it and click **Properties**. The configuration window will appear.

Note

To open the configuration window, you can also check **Open the advanced properties of this task when I click "Finish"** in the last step of the wizard.

Viewing General Information



General

You can see general information about the task (the name, the status, the last time when the task ran). If you want to change the task name, enter a new name in the corresponding field.

If the task is running, you can end the scanning process by clicking **End Task**.

To see the report file on the last task execution, click **View Log**.

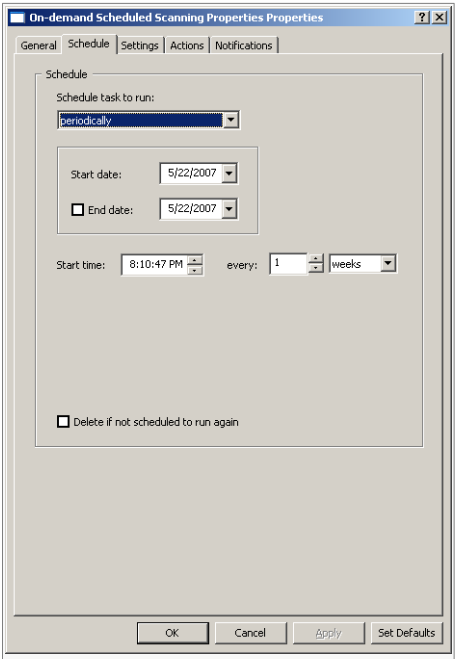
To enable the task, check **Enable Task**. If you want to disable the task, clear the check box.

Click **Apply** to the save changes. If you want to save the changes and close the configuration window, click **OK**.

If you want to close the configuration window without making any changes, click **Cancel**.

Modifying Schedule

Click the **Schedule** tab in the configuration window to modify the schedule.



Schedule

Specify the task schedule.

You must choose one of the following options from the menu:

- **Once** - to run the task one time only, at a given moment.

  Specify the start date and time in the **Start Date / Start Time** fields.

- **Periodically** - to run the task periodically, at certain time intervals (minutes, hours, days, weeks, months, years), starting with a specified date and time.

  To configure the necessary settings, follow these steps:

  1. Specify the start date in the **Start Date** field.
  2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in the corresponding field.

3. Specify the start time in the **Start Time** field.
4. Specify the task frequency by specifying the number of minutes / hours / days / weeks / months / years between two successive occurrences of such task, in the corresponding field..

- **Week Days** - to run the task repeatedly only in certain days of the week starting with a specified date and time.

  To configure the necessary settings, follow these steps:

  1. Specify the start date in the **Start Date** field.
  2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in corresponding field.
  3. Specify the start time in the **Start Time** field.
  4. Specify the day or days of the week on which the task should be run.

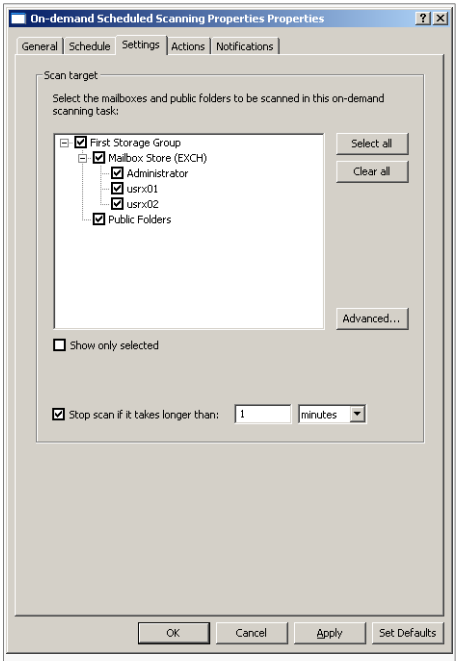
Check **Delete if not scheduled to run again** to delete the task after its last execution.

Click **Apply** to the save changes. If you want to save the changes and close the configuration window, click **OK**.

If you want to close the configuration window without making any changes, click **Cancel**.

Configuring Settings

Click the **Settings** tab in the configuration window to modify the task settings.



Settings

Select Scan Target

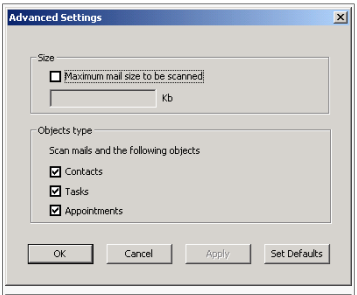
Check the items (groups, mailboxes and public folders) you want to be scanned.

Click **Select All** to check all items. If you click **Clear All** no item will be selected.

If you want to see only the selected items, check **Show only selected**.

Set Advanced Settings

To set advanced scan settings click **Advanced**. A new window will appear.



Advanced Scan Settings

If you do not want to scan messages that exceed a certain size limit, check **Maximum mail size to be scanned** and provide the size limit in the corresponding field.

Beside messages, you can select other objects to be scanned: **Contacts**, **Tasks** and **Appointments**.

If you want to apply the default settings, click **Set Defaults**. Click **OK** to save changes and close the window.

Limit Scanning Time

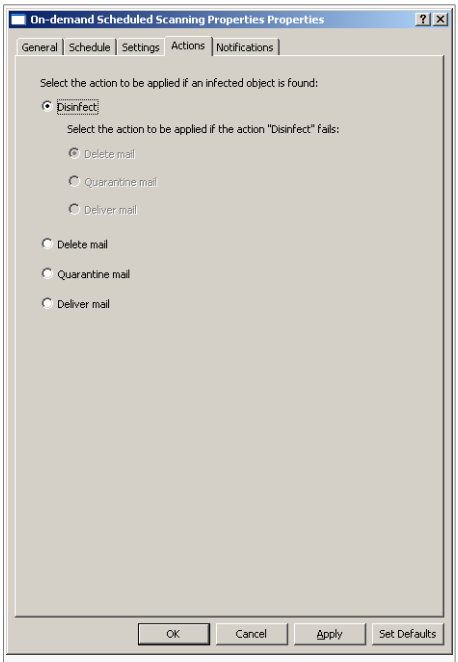
If you want to limit the scanning time, check **Stop scan if it takes longer than** and specify the number of minutes or hours.

Click **Apply** to the save changes. If you want to save the changes and close the configuration window, click **OK**.

If you want to close the configuration window without making any changes, click **Cancel**.

Configuring Action

Click the **Actions** tab in the configuration window to configure the action to be taken on the infected messages.



Notifications

You must choose one of the following actions:

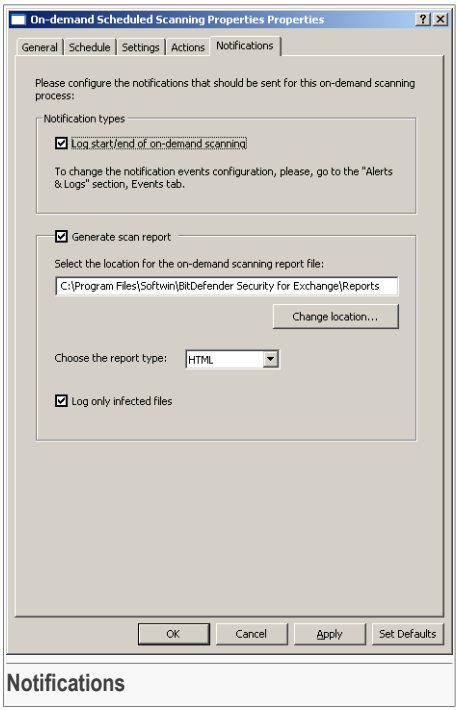
Action	Description
Disinfect	The infected messages are disinfected. You can choose a second action to be taken on the infected messages if disinfection fails. The second action options are delete, quarantine, deliver mail (as defined below).
Delete mail	The infected messages are deleted.
Quarantine mail	The infected messages are moved to the quarantine folder.
Deliver mail	The infected messages are delivered in full to their receivers.

Click **Apply** to the save changes. If you want to save the changes and close the configuration window, click **OK**.

If you want to close the configuration window without making any changes, click **Cancel**.

Configuring Notifications

Click the **Notifications** tab in the configuration window to configure the notifications.



Notifications

Log Scanning

Check **Log start/end of on-demand scanning** to record the start and the end of the process in the log file.

Note

The corresponding event from the Events section must be enabled and properly configured. For more information, please refer to "*Configuring Events*" (p. 57).

Configure Report Settings

Check **Generate Scan Report** to generate a report for the on-demand scan. The default location of the report file is: `C:\Program Files\Softwin\BitDefender Security for Exchange\Reports`. To change this location click **Change location**.

You can choose the format of the report file from the menu. The report can be generated in HTML, text or CSV format.

If you want only the infected / suspect files to be logged in the report, check the corresponding option.

Note

To view the report file, at the end of the scanning process, open the configuration window (select the task and click **Properties**) and then click **View Log**.

Click **Apply** to the save changes. If you want to save the changes and close the configuration window, click **OK**.

If you want to close the configuration window without making any changes, click **Cancel**.

8.4.5. Background Scanning Tasks

Scheduling Tasks

To create a new scheduled task, click **New task**. The configuration wizard will appear. It will guide you through the process of creating a scheduled task.

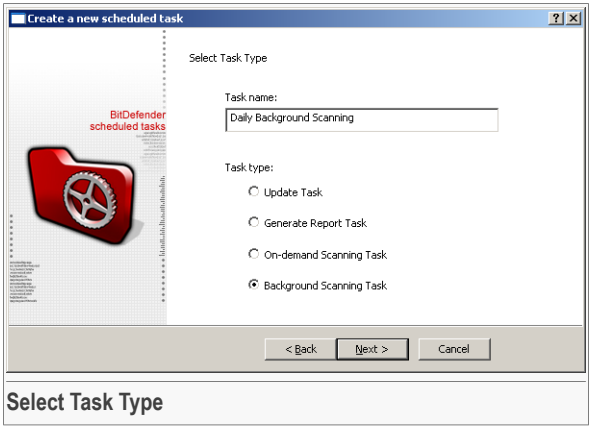
Follow these steps to schedule a background scanning task:

Step 1/4 - Welcome to the Scheduled Tasks Wizard

Welcome

Click **Next**.

Step 2/4 - Select Task Type

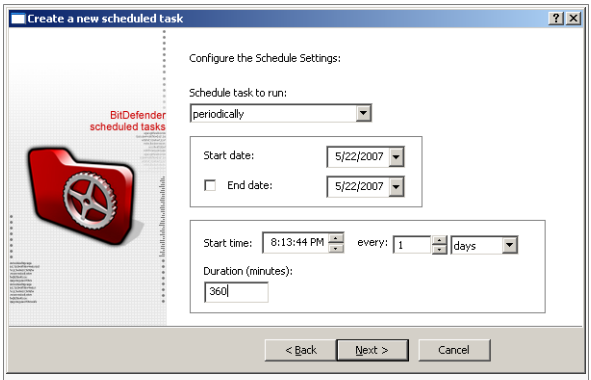


Select Task Type

Provide the task name and then select **Background Scanning Task**.

Click **Next**.

Step 3/4 - Configure Schedule



Run Task Periodically

Specify the task schedule.

You must choose one of the following options from the menu:

- **Once** - to run the task one time only, at a given moment.

  Specify the start date and time in the **Start Date / Start Time** fields.

- **Periodically** - to run the task periodically, at certain time intervals (minutes, hours, days, weeks, months, years), starting with a specified date and time.

  To configure the necessary settings, follow these steps:

  1. Specify the start date in the **Start Date** field.
  2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in the corresponding field.
  3. Specify the start time in the **Start Time** field.
  4. Specify the task frequency by specifying the number of minutes / hours / days / weeks / months / years between two successive occurrences of such task, in the corresponding field..

- **Week Days** - to run the task repeatedly only in certain days of the week starting with a specified date and time.

  To configure the necessary settings, follow these steps:

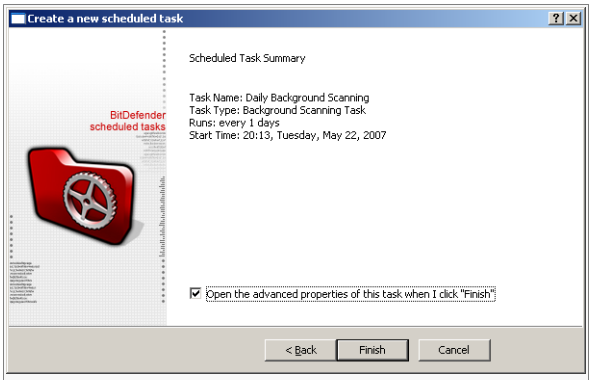
  1. Specify the start date in the **Start Date** field.

2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in corresponding field.
3. Specify the start time in the **Start Time** field.
4. Specify the day or days of the week on which the task should be run.

Specify the duration of the background scanning in the corresponding field.

Click **Next**.

Step 4/4 - View Summary



View Summary

This window allows you to view the task settings and make any changes by returning to the previous steps (**Back**). If you do not want to make any changes, click **Finish**.

Check **Open the advanced properties of this task when I click "Finish"** if you want the **Properties** window of this task to be opened after you complete the wizard. In this window you can modify the task and configure more advanced settings. For more information, please refer to "*Configuring Properties*" (p. 103).

Note

The task will appear in the Scheduled Tasks section.

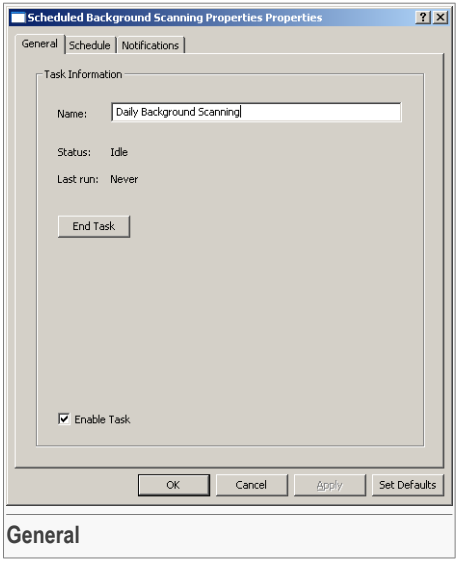
Configuring Properties

In order to modify an existing scheduled task or to configure more advanced settings, unavailable in the configuration wizard, just double-click the task or select it and click **Properties**. The configuration window will appear.

Note

To open the configuration window, you can also check **Open the advanced properties of this task when I click "Finish"** in the last step of the wizard.

Viewing General Information



General

You can see general information about the task (the name, the status, the last time when the task ran). If you want to change the task name, enter a new name in the corresponding field.

If the task is running, you can end the scanning process by clicking **End Task**.

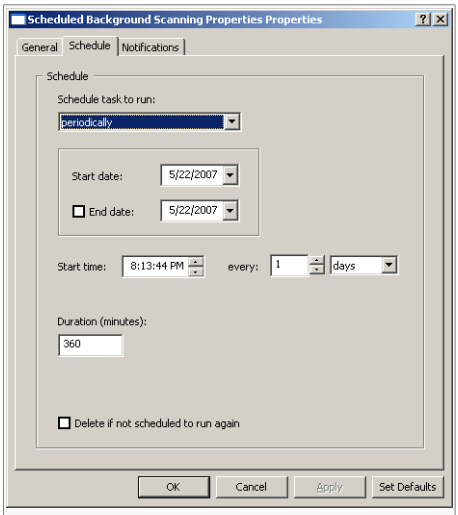
To enable the task, check **Enable Task**. If you want to disable the task, clear the check box.

Click **Apply** to the save changes. If you want to save the changes and close the configuration window, click **OK**.

If you want to close the configuration window without making any changes, click **Cancel**.

Modifying Schedule

Click the **Schedule** tab in the configuration window to modify the schedule.



Schedule

Specify the task schedule.

You must choose one of the following options from the menu:

- **Once** - to run the task one time only, at a given moment.

  Specify the start date and time in the **Start Date / Start Time** fields.

- **Periodically** - to run the task periodically, at certain time intervals (minutes, hours, days, weeks, months, years), starting with a specified date and time.

  To configure the necessary settings, follow these steps:

  1. Specify the start date in the **Start Date** field.
  2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in the corresponding field.
  3. Specify the start time in the **Start Time** field.
  4. Specify the task frequency by specifying the number of minutes / hours / days / weeks / months / years between two successive occurrences of such task, in the corresponding field..

- **Week Days** - to run the task repeatedly only in certain days of the week starting with a specified date and time.

To configure the necessary settings, follow these steps:

1. Specify the start date in the **Start Date** field.
2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in corresponding field.
3. Specify the start time in the **Start Time** field.
4. Specify the day or days of the week on which the task should be run.

Specify the duration of the background scanning in the corresponding field.

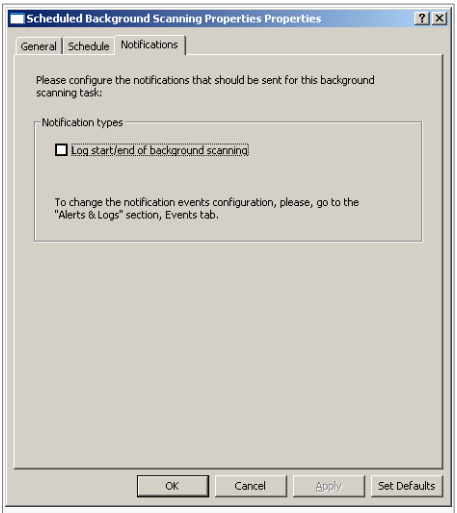
Check **Delete if not scheduled to run again** to delete the task after its last execution.

Click **Apply** to the save changes. If you want to save the changes and close the configuration window, click **OK**.

If you want to close the configuration window without making any changes, click **Cancel**.

Configuring Notifications

Click the **Notifications** tab in the configuration window to configure notifications.



Notifications

Check **Log start/end of background scanning** to keep a record of the start and the end of the background scanning in the log file.

Note

The corresponding event from the Events section must be enabled and properly configured. For more information, please refer to "*Configuring Events*" (p. 57).

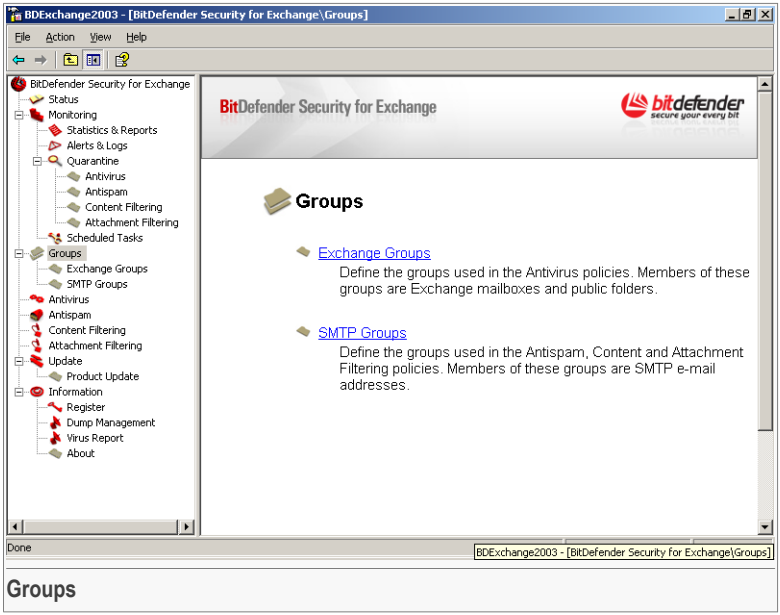
Click **Apply** to the save changes. If you want to save the changes and close the configuration window, click **OK**.

If you want to close the configuration window without making any changes, click **Cancel**.

9. Groups Module

BitDefender allows creating user groups, in order to apply different scanning and filtering policies for different user categories. For example, you can create appropriate policies for the IT department, for the sales team or for the managers of your company.

Click **Groups** in the tree menu to enter this section.



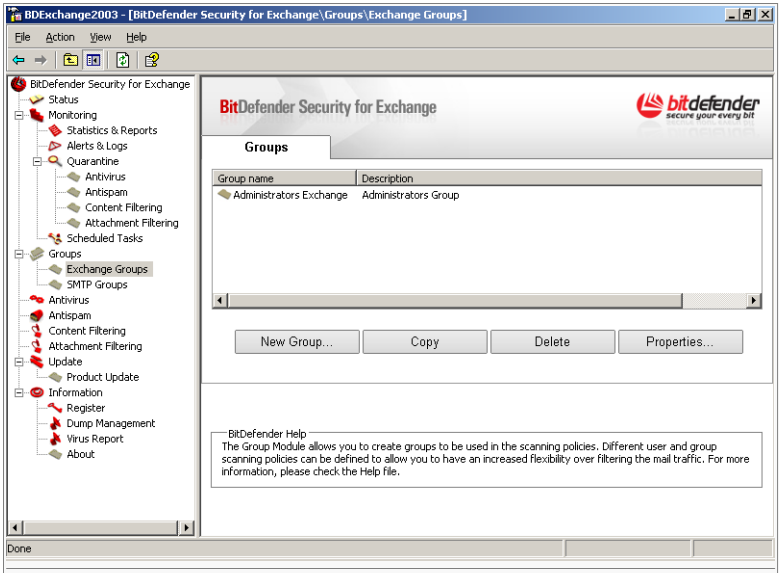
Groups

There are two different kinds of groups:

- Exchange Groups, based on the Exchange mailboxes and used to create antivirus policies.
- SMTP Groups, based on Active Directory and used to create antispam, content and attachment filtering policies.

9.1. Exchange Groups

Click **Exchange Groups** in the tree menu (**Groups** module) to enter this section.



Exchange Groups

This is where you can create and manage Exchange user groups.

Exchange groups contain Exchange users or public folders, organized as on the Exchange server. They are only used to create antivirus scanning policies.

9.1.1. Managing Groups

You can see all the existing groups listed in the table along with their description.

To manage the groups, use the following buttons:

- **New Group** - creates a new group. You will have to configure the group before it appears in the table.
- **Copy** - copies one or several selected groups.
- **Delete** - deletes one or several selected groups. You will have to confirm your choice by clicking **Yes**.

- **Properties** - opens the configuration window of a selected group, allowing you to configure it. To learn how to configure the group, please refer to "*Configuring Exchange Groups*" (p. 111).

9.1.2. Creating Exchange Groups

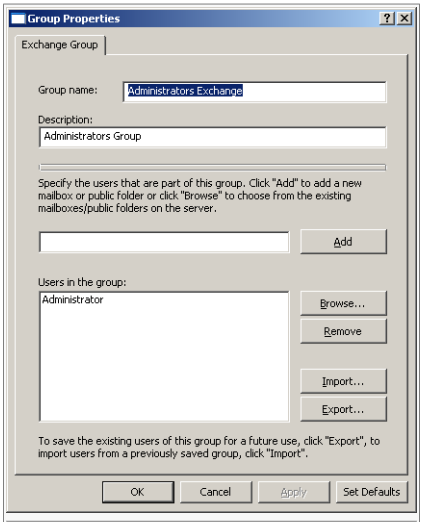
To create a group, choose one of the following methods:

- copy an existing group and click **Properties** to modify it.
- click **New Group** and configure the new group.

In both cases, a configuration window will appear. Next, you must configure the group.

9.1.3. Configuring Exchange Groups

Open the configuration window (select the group and click **Properties**).



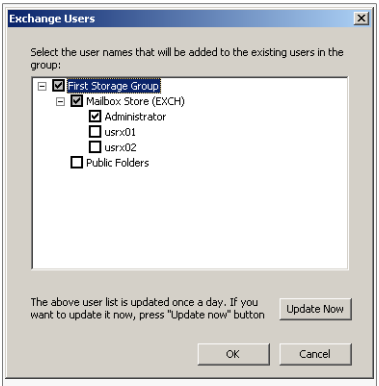
Group Properties

To configure the group follow these steps:

1. **Identify the new group.** Provide the group name and, optionally, the group description in the corresponding fields.

2. **Add users and public folders to the new group.** There are three ways to add items to the group:
   - Provide the user name or the public folder name in the corresponding field and click **Add**.
   - Add users or public folders from the Exchange user list.

     Click **Browse** to search items in the Exchange user list. A new window will appear.



Browse for Users (Groups)

You can see the list of all of your storage groups and the items they contain. A storage group can be empty, it can contain one or more public folders and it can also contain one or more mailbox stores along with their defined items.

The user list is automatically updated once a day. To update the list, click **Update Now**.

Click the box labeled with "+" to show all items contained by an object or the box labeled with "-" to hide the items contained by an object.

Check the items you want to add to the new group and click **OK**.

   - Import the users from a txt file. Click **Import**, select the file and then click **Open** to add the users from the file to the group.

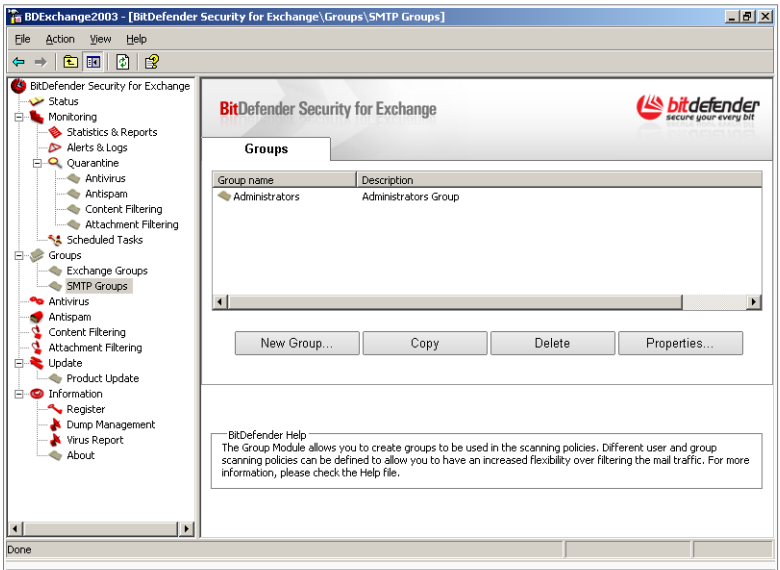
   To remove one or several items from the list, select them, click **Remove** and then **Yes** to confirm your choice.

   You can export the list to a txt file in order to use it when creating other groups. Click **Export** and save the file to the desired location.

3. Click **OK** to save the changes and close the configuration window.

9.2. SMTP Groups

Click **SMTP Groups** in the tree menu (**Groups** module) to enter this section.



SMTP Groups

This is where you can create and manage SMTP groups.

SMTP groups contain users from Active Directory that have an SMTP address assigned. They are used for creating antispam scanning and content and attachment filtering policies.

9.2.1. Managing SMTP Groups

You can see all the existing groups listed in the table along with their description.

To manage the groups, use the following buttons:

- **New Group** - creates a new group. You will have to configure the group before it appears in the table.
- **Copy** - copies one or several selected groups.
- **Delete** - deletes one or several selected groups. You will have to confirm your choice by clicking **Yes**.

- **Properties** - opens the configuration window of a selected group, allowing you to configure it. To learn how to configure the group, please refer to "*Configuring SMTP Groups*" (p. 114).

9.2.2. Creating SMTP Groups

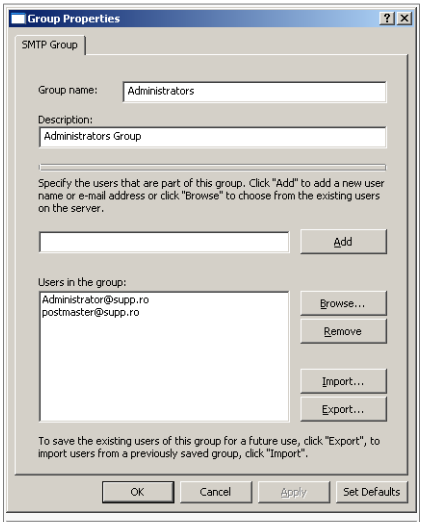
To create a group, choose one of the following methods:

- copy an existing group and click **Properties** to modify it.
- click **New Group** and configure the new group.

In both cases, a configuration window will appear. Next, you must configure the group.

9.2.3. Configuring SMTP Groups

Open the configuration window (select the group and click **Properties**).



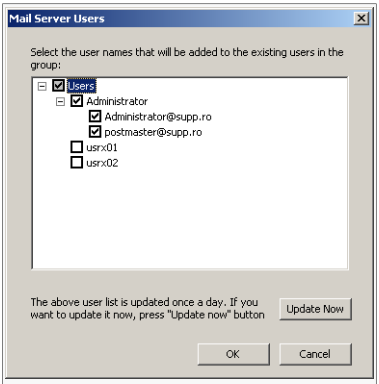
Group Properties

To configure the group follow these steps:

1. **Identify the new group.** Provide the group name and, optionally, the group description in the corresponding fields.

2. **Add users to the new group.** There are three ways to add users to the group:
   - Provide the user name or the e-mail address in the corresponding field and click **Add**.
   - Add users from the Active Directory user list.

     Click **Browse** to search users in the Active Directory user list. A new window will appear.



Browse for Users (Groups)

You can see the list of all the users from Active Directory that have an SMTP address assigned. The list structure is the one from Active Directory.

The user list is automatically updated once a day. To update the list, click **Update Now**.

Click the box labeled with "+" to show all items contained by an object or the box labeled with "-" to hide the items contained by an object.

Check the items you want to add to the new group and click **OK**.

   - Import e-mail addresses from a txt file. Click **Import**, select the file and then click **Open** to add the addresses from the file to the group.

   To remove one or several items from the list, select them, click **Remove** and then **Yes** to confirm your choice.

   You can export the list to a txt file in order to use it when creating other groups. Click **Export** and save the file to the desired location.

3. Click **OK** to save the changes and close the configuration window.

10. Antivirus Module

In the **Antivirus** module you can configure BitDefender to scan messages for viruses and spyware.

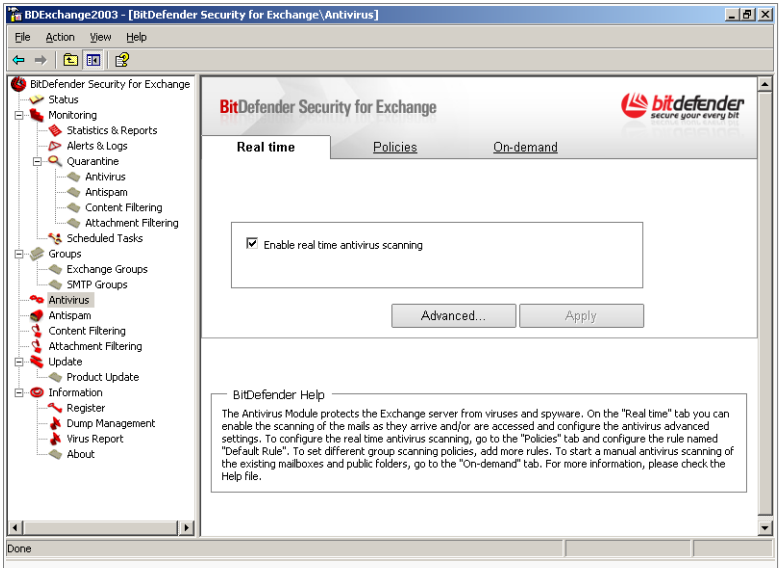
Based on the groups the sender and the receivers belong to, you can specify various actions to be taken on the infected messages.

The module contains two sections:

- Real-time Antivirus Protection - allows you to enable the real-time antivirus protection and to configure advanced settings for the Antivirus module.
- Policies - allows you to configure the scanning options for all incoming mail traffic and to specify different scanning policies based on the groups the sender and the receivers belong to.
- Scan - allows you to configure and initiate on-demand scanning processes.

10.1. Real-time Antivirus Protection

Click **Antivirus** in the tree menu to enter this section.



Real-time Antivirus Protection

This is where you can enable real-time protection and configure advanced antivirus settings.

Check **Enable real time antivirus scanning** to enable the real-time antivirus protection. To disable it, clear the corresponding check box. Click **Apply** to save the changes.

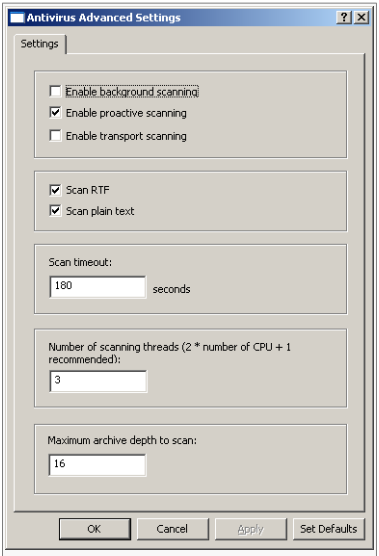
Note

In order to configure the antivirus scanning options for all the incoming mail traffic or to create different scanning policies based on user groups, go to the Policies section.

10.1.1. Configuring Advanced Antivirus Settings

Several advanced settings concerning the scanning process can be configured. These settings are applied regardless of the policy.

Click **Advanced** to open the window where you can configure the advanced settings.



Advanced Antivirus Settings

The following options are available:

- **Enable Background Scanning** - check this option if you want to enable background scanning.

  Background scanning means scanning all folders with a low priority. When an object that has been checked by the background scanning is requested, it will not be scanned again unless a virus definition update has been made. Therefore, enabling this scan method optimizes the overall scanning process.

  To perform background scanning of the messages and attachments, the Information Store will use one thread per database, running at low priority. Once the background scanning is completed, the thread is terminated. This thread is not part of the global virus-scanning thread pool used for on-access scanning.

- **Enable Proactive Scanning** - check this option if you want to enable proactive scanning.

  Proactive scanning means that 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 threads are available in the thread pool and no high priority item remains to be scanned, each item with the low priority is submitted for scanning. Therefore, enabling this scan method optimizes the overall scanning process.

  If an item is on the low priority list and a client attempts to access the message, the item will be marked as high priority. Also, it will be removed from the low priority list and another low priority item will take its place.

  Note

  We recommend you to keep this setting enabled as it prevents the overloading of the scanning engine.

- **Enable Transport Scanning** - check this option if you want to enable transport scanning.

  Note

  Transport scanning is available only on MS Exchange Server 2003!

  Transport scanning means that messages are scanned at the transport level. This prevents infected messages from entering the Exchange organization.

  The messages entering the Exchange store are intercepted by the VS API interface and scanned by BitDefender. After being scanned, the messages are submitted again to the transport engine which will deliver them to their destination. Any message scanned at the gateway will be rescanned on the back-end server.

  Note

  We recommend enabling transport scanning only when BitDefender Security for Exchange is installed on a gateway.

- **Scan RTF** - check this option if you want the body messages in RTF (Rich Text Format) to be scanned.
- **Scan Plain Text** - check this option if you want the body messages in plain text format to be scanned.

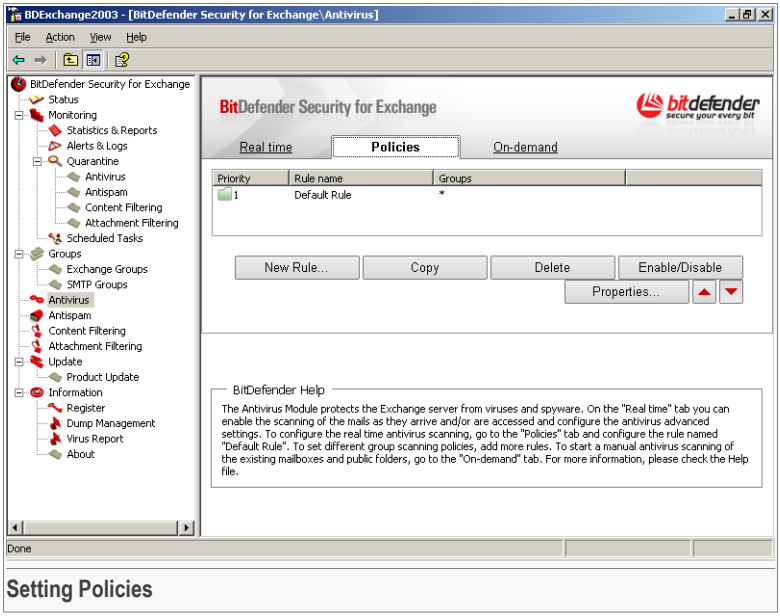
- **Scan Timeout** - provide in the corresponding field the maximum time allocated to scan an object. If the scanning process is not completed before the timeout interval, an error is returned and access to the object is denied.
- **Number of threads** - provide in the corresponding field the maximum number of threads to be used. The recommended number can be computed this way: `2*number of CPU+1`.
- **Maximum archive depth to scan** - provide in the corresponding field the maximum archive depth to scan. The recommended depth is 16.

  Archives can contain other archives. It is possible to find files with multiple archive levels. If there are too many such levels, the scanning process can take longer, affecting the performance of the server. It is advisable to set a maximum level up to which the archives are to be scanned.

Click **OK** to save the changes. If you want to restore the default settings, click **Set Defaults**.

10.2. Setting Policies

Click **Antivirus** in the tree menu and then the **Policies** tab to enter this section.



Setting Policies

This is where you can configure the rules for the real-time antivirus scanning.

10.2.1. Managing Rules

You can see all the existing rules listed in the table. For each rule, the following information is provided: priority, the name and the groups of senders and receivers it applies to. The rules are listed by order of priority with the first rule counting as the highest priority.

Note

Messages are checked against each rule, by order of priority, until the sender and the receivers of the message match a rule. The message is then processed according to the antivirus scanning options specified by that rule.
Please note that messages can be scanned before the rule is applied, by the transport (only for MS Exchange Server 2003), proactive or background scanning, regardless of the policy.

- If the message was not scanned before the client's request, it is scanned according to the rule.
- If the message was checked before by proactive or background scanning and no update was performed in the meantime, the message is delivered without being scanned according to the rule.
- If the message was checked before by proactive or background scanning but an update was performed in the meantime, the message is scanned according to the rule.
- Only for MS Exchange Server 2003! If the message was previously scanned at transport level, it is also scanned according to the rule.

For more information, please refer to "*Configuring Advanced Antivirus Settings*" (p. 119).

Default Rule. There is one rule created by default that manages the real-time antivirus scanning settings for all groups. You can neither copy, delete or disable this rule. The default rule has the lowest priority; therefore, you cannot change its priority. Because the rule was designed to apply to the entire mail traffic, you cannot configure group options. However, you can configure all the other options.

Group Filtering Policies. To set different antivirus policies, add new rules. This way you can create customized filtering rules for the mail traffic between certain groups of users.

To manage the rules, use the following buttons:

- **New** - creates a new rule. You will have to configure the rule before it appears in the table.
- **Copy** - copies one or several selected rules.
- **Delete** - deletes one or several selected rules. You will have to confirm your choice by clicking **Yes**.
- **Enable / Disable** - enables or disables one or several selected rules.
- **Properties** - opens the configuration window of a selected rule, allowing you to modify the rule. To learn how to configure the rule, please refer to "*Configuring Rules*" (p. 124).
- **Up** - moves a selected rule one level up in the table. This will increase the priority of the rule.
- **Down** - moves a selected rule one level down in the table. This will decrease the priority of the rule.

10.2.2. Creating Rules

To create a rule, choose one of these methods:

- copy an existing rule and click **Properties** to modify it.
- click **New Rule** and configure the new rule.

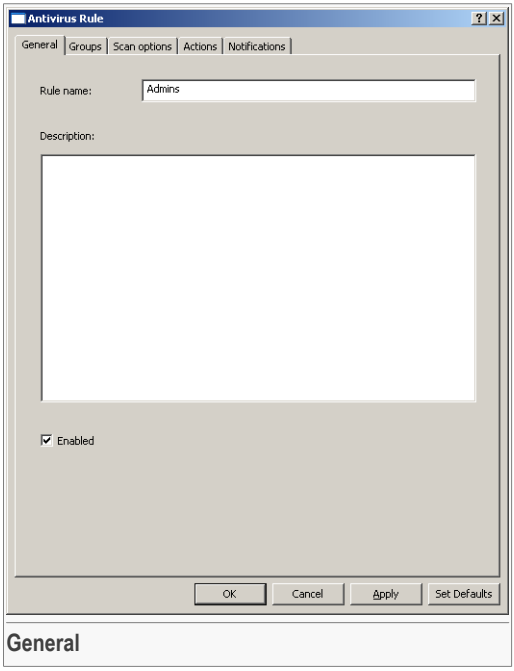
In both cases, a new window will appear. Next, you must configure or modify the rule.

10.2.3. Configuring Rules

To configure a rule follow these steps:

Step 1/5 - Provide General Data

Open the configuration window and provide general data for the rule.



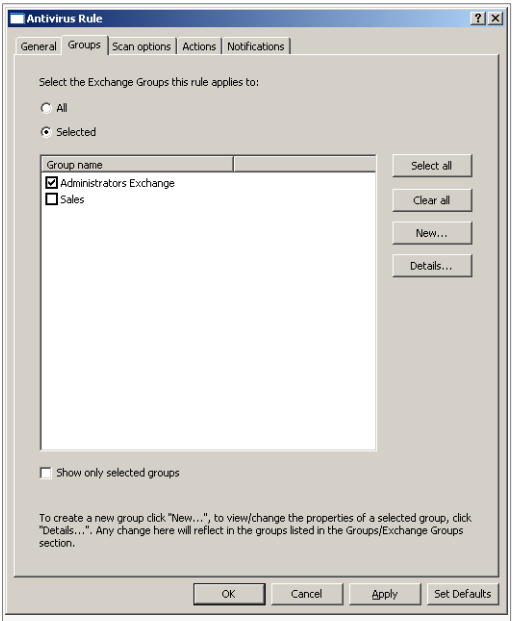
General

Provide the rule name and, optionally, the rule description.

To enable the rule, check **Enabled**. If you want the rule to be disabled, clear the check box.

Step 2/5 - Select Groups

Click the **Groups** tab and select the Exchange groups the rule applies to.



Groups

The following options are available:

- **All** - the rule applies to all the Exchange mailboxes and public folders.
- **Selected** - the rule applies only to the selected Exchange mailbox groups.

If you choose **Selected**, you have to check the groups from the list you want the rule to apply to.

Click **Select All** to check all groups. If you click **Clear All** no group will be selected.

If needed, you can create a new Exchange group by clicking **New** and configuring it. The new group will appear in the Exchange Groups section.

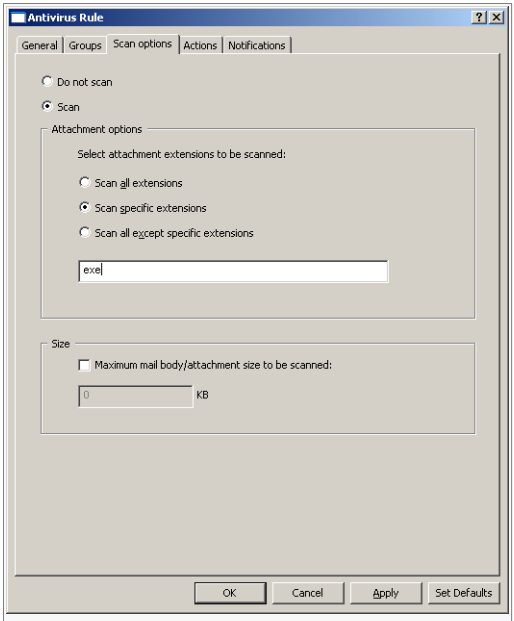
To configure an existing group or to see its parameters, select it and click **Details**.

Note

To learn how to configure an Exchange group, check the "*Creating Exchange Groups*" (p. 111) section of this user guide.

Step 3/5 - Configure Scan Options

Click the **Scan Options** tab and configure the scan options for the messages matching this policy.



Scan Options

If you do not want to scan the messages for malware, select **Do not scan**. Then, click **OK** to save the changes and close the configuration window.

If you select **Scan**, the messages will be scanned for malware using the settings configured for this policy. The following options are available:

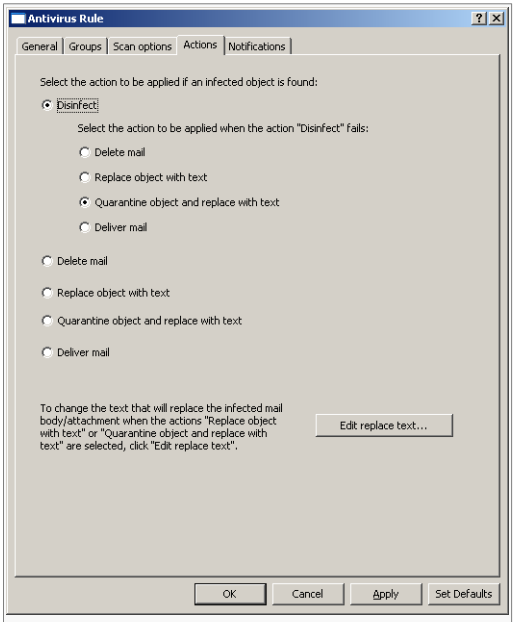
- **Attachment extensions to be scanned** - select one of the following options in order to scan attachments depending on their extension.

Option	Description
Scan all extensions	All mail attachments are scanned, regardless of their extension.
Scan specific extensions	Only the attachments having the specified extensions are scanned. Provide the specific extensions in the edit field. These extensions must be separated by ";".
Scan all except specific extensions	All attachments except those having the specified extensions are scanned. Provide the extensions excepted from scanning in the edit field. These extensions must be separated by ";".

- **Maximum mail body / attachment size to be scanned** - check this option if you want to specify a size limit for the mail body or for the attachments to be scanned. Provide the size limit in the edit field.

Step 4/5 - Set Actions

Click the **Actions** tab and specify the action to be taken on the infected messages.



Actions

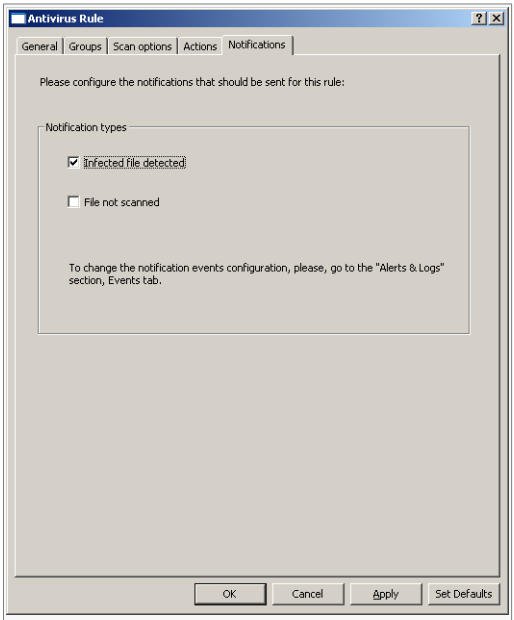
You must choose one of the following actions:

Action	Description
Disinfect	The infected message is disinfected. You can choose a second action to be taken on the infected messages if disinfection fails. The second action options are delete, quarantine, deliver mail (as defined below).
Delete mail	The infected message is deleted.
Replace object with text	The infected object (mail body / attachment) is replaced with a specified text. To specify the text to be delivered instead of the content of the infected object click **Edit Replace Text**. Provide the text in the edit box that appears and click **OK**.

Action	Description
Quarantine object and replace with text	The infected object (mail body / attachment) is moved to the quarantine folder and its content is replaced with a specified text. To specify the text to be delivered instead of the content of the infected object click **Edit Replace Text**. Provide the text in the edit box that appears and click **OK**.
Deliver mail	The infected message is delivered in full to its receivers.

Step 5/5 - Configure Notifications

Click the **Notifications** tab and specify whether to issue notifications or not when infected messages are detected or files cannot be scanned.



Notifications

Check the events for which to issue notifications:

- **Infected file detected** - when an infected file was detected.
- **File not scanned** - when a file could not be scanned.

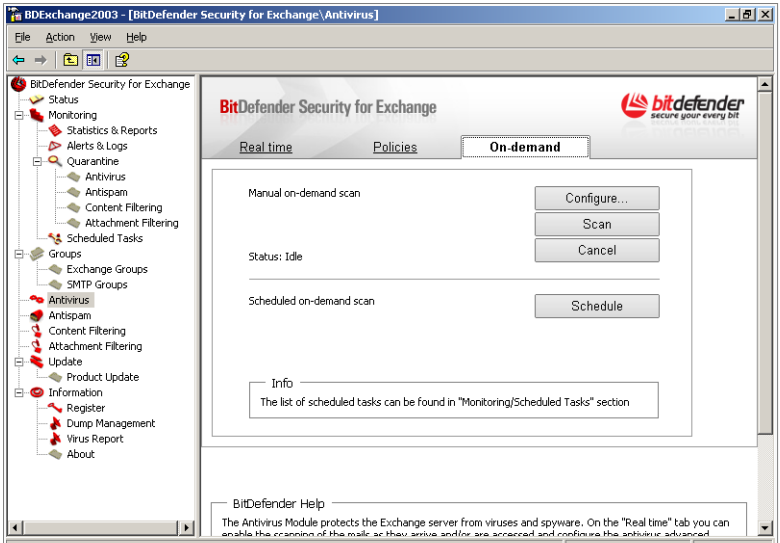
Note

The corresponding event in the Events section must be enabled and properly configured. For more information, please refer to "*Configuring Events*" (p. 57).

Click **OK** to save the changes and close the configuration window.

10.3. On-demand Scanning

Click **Antivirus** in the tree menu and then the **On-demand** tab to enter this section.



On-demand Scanning

This is where you can configure and initiate on-demand scanning processes.

BitDefender can scan on-demand the existing mailboxes and public folders for viruses and spyware.

In order to perform an on-demand scan, you must configure the scan settings and then click **Scan**. You can stop the scan process anytime you want by clicking **Cancel**.

Note

Only one on-demand scan can be run at a time.

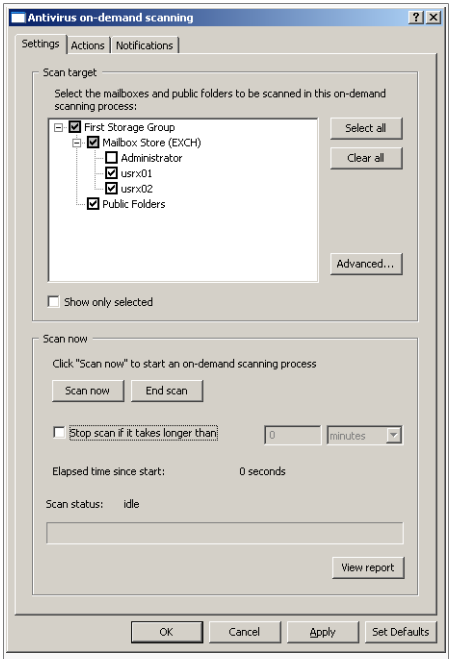
If you want to schedule an on-demand scan, click **Schedule** and follow the steps of the wizard. For more information, please refer to "*On-demand Scanning Tasks*" (p. 86).

10.3.1. Configuring Scan Settings

Click **Configure** to open the window where you can configure the settings for the on-demand scan. Follow these steps to configure the scan settings:

Step 1/3 - Configure Scan Settings

Specify the scan target and other scan settings.



On-demand Scan Settings

Select Scan Target

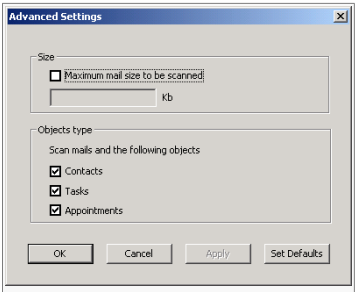
Check the items (groups, mailboxes and public folders) you want to be scanned.

Click **Select All** to check all items. If you click **Clear All** no item will be selected.

If you want to see only the selected items, check **Show only selected**.

Set Advanced Settings

To set advanced scan settings click **Advanced**. A new window will appear.



Advanced Scan Settings

If you do not want to scan messages that exceed a certain size limit, check **Maximum mail size to be scanned** and provide the size limit in the corresponding field.

Beside messages, you can select other objects to be scanned: **Contacts**, **Tasks** and **Appointments**.

If you want to apply the default settings, click **Set Defaults**. Click **OK** to save changes and close the window.

Scanning

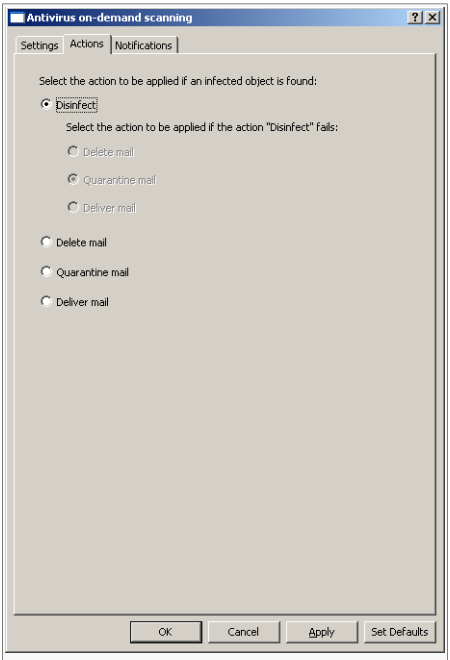
To start scanning, just click **Scan Now**. You can stop the scan process anytime you want to by clicking **End Scan**.

If you want to limit the scanning time, check **Stop scan if it takes longer than** and specify the number of minutes or hours.

At the end of the scanning process, return to this section and click **View Report** to view the report file.

Step 2/3 - Set Action

Click the **Actions** tab and specify the action to be taken on the infected messages.



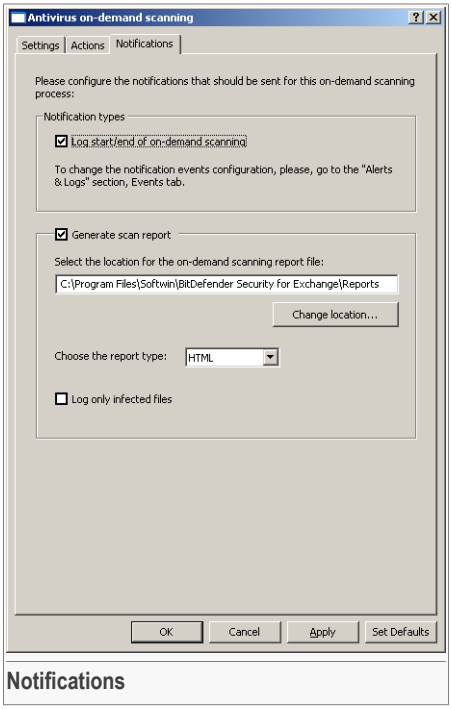
Scan Action

You must choose one of the following actions:

Action	Description
Disinfect	The infected messages are disinfected. You can choose a second action to be taken on the infected messages if disinfection fails. The second action options are delete, quarantine, deliver mail (as defined below).
Delete mail	The infected messages are deleted.
Quarantine mail	The infected messages are moved to the quarantine folder.
Deliver mail	The infected messages are delivered in full to their receivers.

Step 3/3 - Configure Notifications

Click the **Notifications** tab and configure the notifications issued for the on-demand scan.



Notifications

Log Scanning

Check **Log start/end of on-demand scanning** to record the start and the end of the process in the log file.

Note

The corresponding event from the Events section must be enabled and properly configured. For more information, please refer to "*Configuring Events*" (p. 57).

Configure Report Settings

Check **Generate Scan Report** to generate a report for the on-demand scan. The default location of the report file is: `C:\Program Files\Softwin\BitDefender Security for Exchange\Reports`. To change this location click **Change location**.

You can choose the format of the report file from the menu. The report can be generated in HTML, text or CSV format.

If you only want the infected / suspect files to be logged in the report, check the corresponding option.

Note

To view the report file, at the end of the scanning process, open this configuration window and click **View Report** in the **Settings** section.

Click **OK** to save the changes and close the configuration window.

11. Antispam Module

The **Antispam** module offers protection against spam, phishing and other attacks. It uses a combination of various filters and engines to determine whether messages are spam or not and to check them for patterns of spam.

Based on the groups the sender and the receivers belong to, you can specify various actions to be taken on the spam messages.

The module contains two sections:

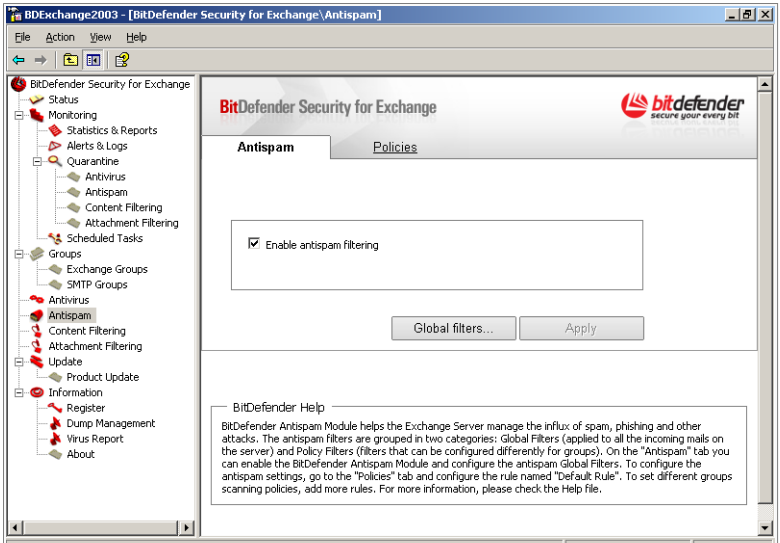
- Antispam Filtering - allows you to enable the Antispam Filtering and to configure the global antispam filters.
- Policies - allows you to configure the filtering options for all incoming mail traffic and to specify different filtering policies based on the groups the sender and the receivers belong to.

Note

Antispam Filtering is available only for MS Exchange 2000/2003.

11.1. Antispam Filtering

Click **Antispam** in the tree menu to enter this section.



Antispam Filtering

This is where you can enable antispam filtering and configure the global antispam filters.

Check **Enable Antispam Filtering** to enable the antispam protection. To disable it, clear the corresponding check box. Click **Apply** to save the changes.

Note

In order to configure the antispam filtering options for all the incoming mail traffic or to create different filtering policies based on user groups, go to the Policies section.

11.1.1. Configuring Global Antispam Filters

Several filters can be configured to filter all of the incoming mail traffic, in order to reduce the traffic on the server. These filters are used when scanning messages regardless of the policy.

Note

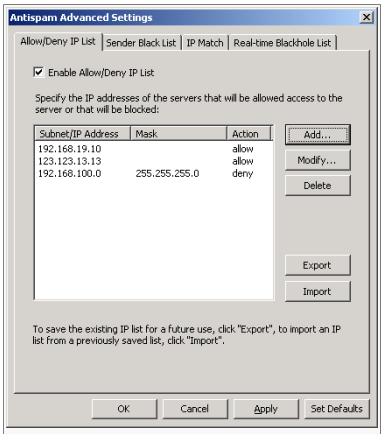
We recommend you to configure these filters when BitDefender Security for Exchange is installed on a gateway.

Click **Global Filters** to open the configuration window.

Follow these steps to configure the global antispam filters:

Step 1/4 - Configure Allow / Deny IP List

Open the configuration window to configure the Allow / Deny IP List.



Allow / Deny IP List

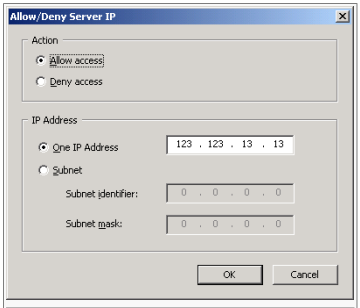
The Allow / Deny IP List enables the administrator to specify IP addresses which are denied access to the server. All incoming connections from addresses that appear on the Deny IP List are dropped, provided that such addresses do not appear on the Allow IP List.

Note

The Allow IP List is used to except IP addresses from ranges of IP addresses defined on the Deny IP List.

Check **Enable Allow / Deny IP List** and configure the IP addresses if you want to use the Allow / Deny IP List to filter the incoming mail traffic.

Add IP Addresses. Click **Add** to add a new IP address to the list. The configuration window will appear.



Add IP Address

Follow these steps to configure a new entry on the IP list:

1. Choose the action to be applied to the mail traffic coming from the specified IP address: **Allow access** or **Deny access**.
   - If you select **Deny access**, the incoming connection from the specified IP addresses will be dropped.
   - If you select **Allow access**, messages coming from the specified IP addresses will be allowed to pass.
2. Provide the IP addresses to which the action will apply.
   - If you want to enter a single IP address, select **One IP address** and provide it in the corresponding field.
   - If you want to enter a range of IP addresses, select **Subnet** and provide the subnet identifier and the subnet mask in the corresponding fields.
3. Click **OK** to add the entry to the IP list.

Manage IP List. You can see the IP addresses and the associated action listed in the table. If you want to modify an entry, either double-click it or select it and click **Modify**. To remove one or several selected entries, click **Remove** and then **Yes** to confirm your choice.

Import / Export IP List. To export the IP list to a `txt` file, click **Export** and save the file to the desired location. To import a previously saved list, click **Import**.

Step 2/4 - Configure Sender Black List

Click the **Sender Black List** tab to configure the Sender Black List filter.

Sender Black List

The Sender Black List allows the administrator to specify a list of e-mail addresses which are denied access to the server. The incoming mail from these addresses will be dropped before reaching the server.

Check **Enable Sender Black List** and add the banned addresses if you want to use the Sender Black List to filter incoming mail traffic.

Add Addresses. Click **Add** to add a new address to the list. Provide the address in the window that will appear and then click **OK**.

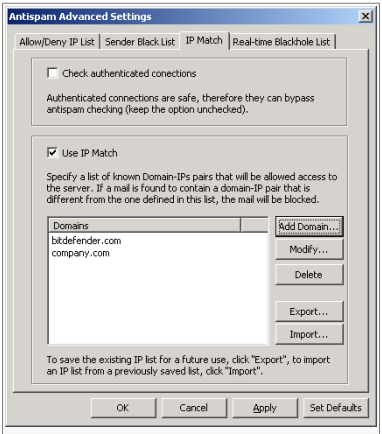
Manage Addresses. You can see the e-mail addresses listed in the table. If you want to modify an address, either double-click it or select it and click **Modify**. To remove one or several selected addresses, click **Delete** and then **Yes** to confirm your choice.

Import / Export Addresses. To import addresses from a `txt` file, click **Import**, select it and then click **Open**. To export the existing addresses to a `txt` file, click **Export** and save the file to the desired location. This way you can use the address list when configuring BitDefender server products on other machines or after reinstalling the product.

Click **OK** to save the changes and close the window. If you click **Cancel** all changes will be lost.

Step 3/4 - Configure IP Match

Click the **IP Match** tab to configure the IP Match filter.



IP Match

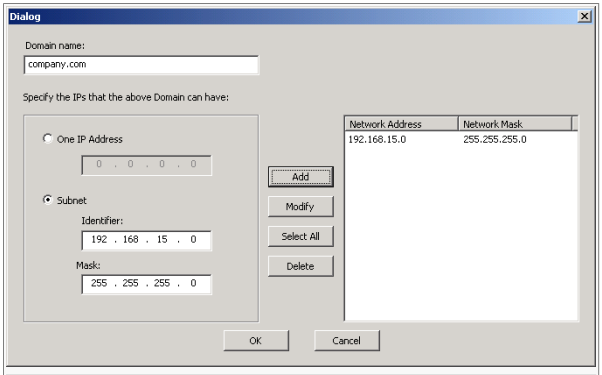
Microsoft Exchange Server 2003 allows authenticating connections. Connections that are authenticated are trusted, therefore they should be allowed to bypass spam detection. However, you can set BitDefender to scan the incoming mail traffic from authenticated sources by selecting **Check authenticated connections**.

Spammers often try to "spoof" the sender's e-mail address to make the e-mail appear as being sent by someone in your domain. To prevent this, you can use IP Match.

If an e-mail appears to be from a domain that you have specified in the IP Match rule list (such as your own company domain), BitDefender checks to see if the IP address of the sender matches the IP addresses provided for the specified domain. If the domain address of the sender matches the IP address, the message bypasses antispam filtering. Otherwise, the connection is dropped.

Check **Use IP Match** and configure the rule list if you want to filter incoming mail traffic using IP Match.

Add Rules. Click **Add** to add a new rule to the list. The configuration window will appear.



Adding Rules

Follow these steps to configure a rule:

1. Provide the domain name in the corresponding field.
2. Provide the IP addresses associated with the specified domain.
   - If you want to enter a single IP address, select **One IP address** and provide it in the corresponding field. Click **Add** to add the entry to the list.
   - If you want to enter a range of IP addresses, select **Subnet** and provide the subnet identifier and the subnet mask in the corresponding fields. Click **Add** to add the entry to the list.

   In the table on the right, you can see the IP addresses as they are added. If you want to modify an existing entry, select it, make the necessary changes and click **Modify**.

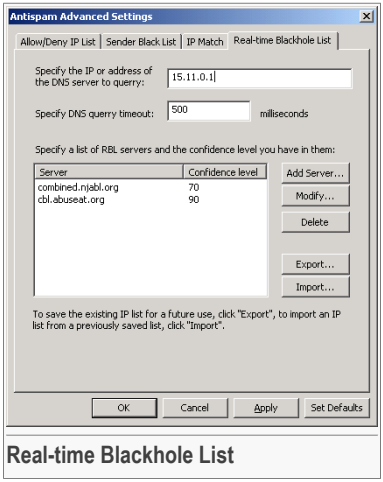
   To select all entries, just click **Select All**. To delete one or several entries from the list, select them and click **Remove** and then **Yes** to confirm your choice.
3. Click **OK** to add the rule to the list.

Manage Rules. You can see the existing rules listed in the table. If you want to modify a rule, either double-click it or select it and click **Modify**. To remove one or several selected rules, click **Remove** and then **Yes** to confirm your choice.

Import / Export Rule List. To export the rule list to a `txt` file, click **Export** and save the file to a desired location. To import a previously saved list, click **Import**.

Step 4/4 - Configure Real-time Blackhole List

Click the **Real-time Blackhole List** to configure this filter.



Real-time Blackhole List

The Real-time Blackhole List (RBL) filter allows checking the mail server from which a message is sent against the RBL servers configured by the administrator. It uses the DNSBL protocol and RBL servers to filter spam based on mail servers' reputation as spam senders.

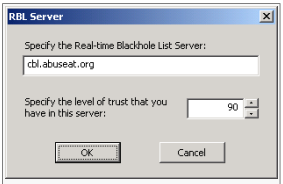
A DNS check is performed on the domain `d.c.b.a.rbl.example.com`, where `d.c.b.a` is the reversed IP address of the server and `rbl.example.com` is the RBL server. If the DNS replies that the domain is valid, it means that the IP is listed in the RBL server and a certain server score is provided. This score ranges between 0 and 100, according to the configured server confidence (trust level).

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

If the RBL filter score is 100 or higher, the message is considered SPAM and the specified action is taken. Otherwise, a spam score is computed from the RBL filter score and added to the global spam score of the message.

Provide the IP or the address of the DNS server to query and the query timeout interval in the corresponding fields.

Add RBL Servers. Click **Add** to add a new RBL server to the list. The configuration window will appear.



Add RBL Servers

First, specify the name of the RBL server and then the level of trust. The level of trust is an indicator on a scale from 0 to 100 which shows the accuracy you consider the RBL server to have. The value you provide is used when computing the SPAM score. Click **OK** to add the RBL server to the list.

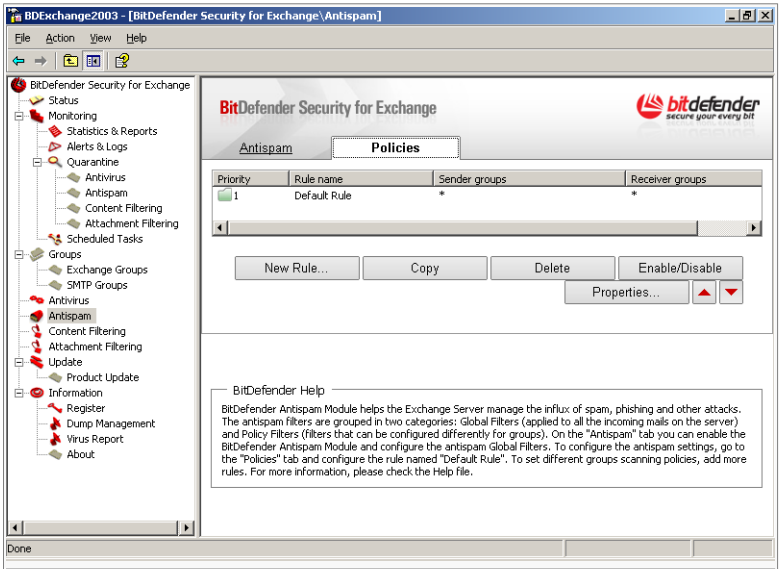
Manage RBL Servers. You can see the RBL servers listed in the table. If you want to modify the settings for an RBL server, either double-click it or select it and click **Modify**. To remove one or several selected RBL servers, click **Remove** and then **Yes** to confirm your choice.

Import / Export RBL Servers. To export the existing RBL servers and their settings to a `txt` file, click **Export** and save the file to the desired location. To import a previously saved database of RBL servers click **Import**.

Click **OK** to save the changes and close the configuration window.

11.2. Setting Policies

Click **Antispam** in the tree menu and then the **Policies** tab to enter this section.



Setting Policies

This is where you can specify the antispam filtering options. You can modify the default rule to specify the antispam filtering options for all the mail traffic, or you can configure new rules in order to create customized group filtering policies.

11.2.1. Managing Rules

You can see all the existing rules listed in the table. For each rule, the following information is provided: priority, the name and the groups of senders and receivers it applies to. The rules are listed by order of priority with the first rule counting as the highest priority.

Note

Messages are checked against each rule, by order of priority, until the sender and the receivers of the message match a rule. The message is then processed according to the antispam filtering options specified by that rule.

Please note that the mail traffic is first filtered using the global antispam filters. The messages that pass the global filters are then checked against the existing policies. For more information, please refer to "*Configuring Global Antispam Filters*" (p. 138).

Default Rule. There is one rule created by default that manages the antispam filtering settings for all groups. You cannot copy, delete or disable this rule. The default rule has the lowest priority; therefore, you cannot change its priority. Because the rule was designed to apply to the entire mail traffic, you cannot configure group options. However, you can configure all the other options.

Group Filtering Policies. To set different filtering policies, add new rules. This way you can create customized filtering rules for the mail traffic between certain groups of users.

To manage the rules, use the following buttons:

- **New Rule** - creates a new rule. You will have to configure the rule before it appears in the table.
- **Copy** - copies one or several selected rules.
- **Delete** - deletes one or several selected rules. You will have to confirm your choice by clicking **Yes**.
- **Enable / Disable** - enables or disables one or several selected rules.
- **Properties** - opens the configuration window of a selected rule, allowing you to modify the rule. To learn how to configure the rule, please refer to "*Configuring Rules*" (p. 147).
- **Up** - moves a selected rule one level up in the table. This will increase the priority of the rule.
- **Down** - moves a selected rule one level down in the table. This will decrease the priority of the rule.

11.2.2. Creating Rules

To create a rule, choose one of these methods:

- copy an existing rule and click **Properties** to modify it.
- click **New Rule** and configure the new rule.

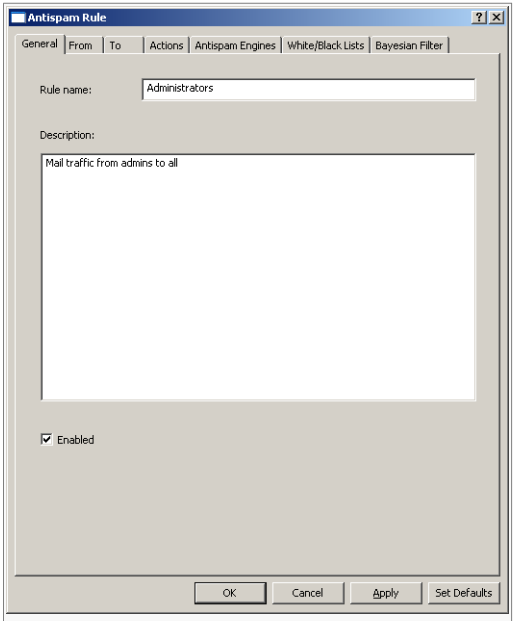
In both cases, a new window will appear. Next, you must configure or modify the rule.

11.2.3. Configuring Rules

To configure a rule follow these steps:

Step 1/7 - Provide General Data

Open the configuration window and provide general data for the rule.



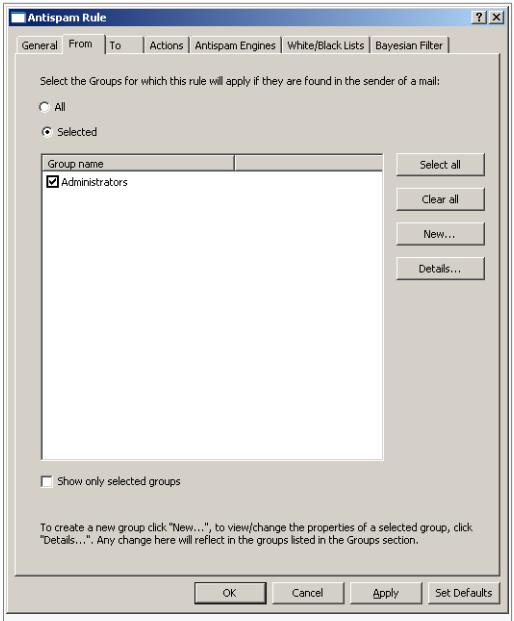
General

Provide the rule name and, optionally, the rule description.

To enable the rule, check **Enabled**. If you want the rule to be disabled, clear the check box.

Step 2/7 - Select Senders Groups

Click the **From** tab and select the groups of senders the rule applies to.



Senders Groups

The following options are available:

- **All** - the rule applies to all senders, no matter if they belong to a group or not.
- **Selected** - the rule applies only to receivers from the selected SMTP groups.

If you choose **Selected**, you have to check from the list the groups you want the rule to apply to.

Click **Select All** to check all groups. If you click **Clear All** no group will be selected.

If necessary, you can create a new SMTP group by clicking **New** and configuring it. The new group will appear in the SMTP Groups section.

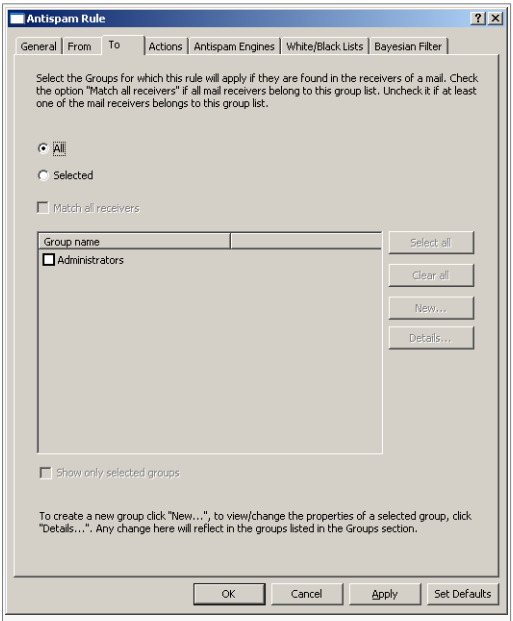
To configure an existing group or to see its parameters, select it and click **Details**.

Note

To learn how to configure an SMTP group, please refer to "*Creating SMTP Groups*" (p. 114).

Step 3/7 - Select Receivers Groups

Click the **To** tab and select the groups of receivers the rule applies to.



Receivers Groups

The following options are available:

- **All** - the rule applies to all receivers, no matter if they belong to a group or not.
- **Selected** - the rule applies only to receivers from the selected SMTP groups.

If you choose **Selected**, you have to check from the list the groups you want the rule to apply to.

You can check the **Match all receivers** option to apply the rule only if all the receivers of the message belong to the specified groups. For example, if the e-mail is sent to

several receivers and at least one of them is not found in the specified groups, the rule will not apply.

Note

The addresses in the **Cc** and **Bcc** fields also count as receivers.

Click **Select All** to check all groups. If you click **Clear All** no group will be selected.

If necessary, you can create a new SMTP group by clicking **New** and configuring it. The new group will appear in the SMTP Groups section.

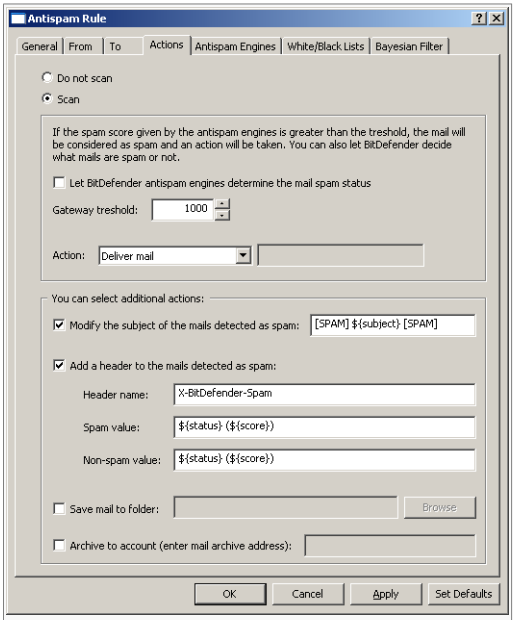
To configure an existing group or to see its parameters, select it and click **Details**.

Note

To learn how to configure an SMTP group, please refer to "*Creating SMTP Groups*" (p. 114).

Step 4/7 - Set Actions

Click the **Actions** tab and specify the actions to be taken on the messages matching this policy.



Actions

If you do not want to scan the messages using the antispam filters, select **Do not scan**. Then, click **OK** to save the changes and close the configuration window.

If you select **Scan**, the messages will be scanned using the antispam filters and the antispam options configured for this policy. Next, you must configure the threshold level and the actions to be taken on the spam messages.

Specify Threshold Level

BitDefender checks all the message components (i.e. not only the header but also the message body in either HTML or text format) against many rules, using several filters. Some of the filters, like the URL Filter, the Image Filter and others, can indicate if the message is spam directly.

The Bayesian Filter, the Pre-trained Bayesian Filter and the NeuNet Filter give to each scanned message a Spam score. The aggregate of these scores represents an overall spam score.

The overall spam score is measured against the desired level of spam sensitivity (threshold), and a decision is made. If the spam score for a message exceeds the threshold, the message is considered spam. Otherwise, the message is not spam and it is delivered in full to its receivers.

Note

Exceptions are made if the sender is in the IPMatch table (as not spam) or on the White list.

Specify a threshold value between 0 and 1000 in the corresponding field. The default value is 775.

If you do not want to set a threshold value, check **Let BitDefender antispam engines determine the mail spam status** to let the BitDefender Antispam Engine to decide whether a message is spam or not.

Set Actions

Choose from the menu one of the following actions to be taken on the spam messages:

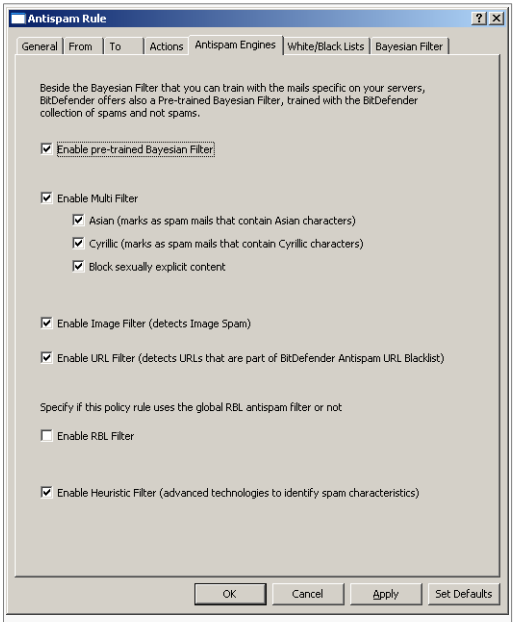
Action	Description
Deliver mail	The spam message is delivered in full to its receivers.
Delete mail	The spam message is deleted.
Quarantine	The spam message is moved to the quarantine folder.
Redirect mail to address	The spam message is redirected to a specified e-mail address. You must specify the e-mail address where the spam messages will be delivered in the field next to the menu. If you want to provide more than one address, separate them by a semi-colon ";". If the field is empty or the e-mail address is invalid the messages will not be redirected.
Reject mail	The spam message is rejected with a 550 SMTP error code.

In order to help you process spam messages, several additional actions are available:

Action	Description
Modify the subject of the mails detected as spam	The subject of the messages detected as spam is modified. You can modify the subject pattern. We recommend you to use one of these patterns: • `[SPAM]${subject}[SPAM]` - to add `[SPAM]` before and after the subject. This is the default subject pattern. • `[SPAM]` - to replace the subject with `[SPAM]`. • `[$score% SPAM]$subject` - to add `[x SPAM]` before the subject, where `x` represents the spam score.
Add a header to the mails detected as spam	An e-mail header is added to the messages detected as spam. You can modify the header name and the spam and non-spam values. By default, the spam and non-spam values are `${status} (${score})`. This means that for a spam message the header will be `Name: Yes(x)`, while for a legitimate message the header will be `Name: No(x)`, where `x` represents the spam score received by the message.
Save mail to folder	The spam message is saved to a specified folder. To specify the folder, click **Browse**, locate it and then click **OK**.
Archive to account	The spam message is archived to a specified account. Provide the e-mail archive address in the field next to this option. A Bcc containing the address will be added to the detected message.

Step 5/7 - Configure Antispam Engines

Click the **Antispam Engines** tab and specify which antispam engines to be enabled.



Antispam Engines

Note

For more information on the antispam filters mentioned here, please refer to "*Policy Filters*" (p. 20).

The following options are available:

- **Enable pre-trained Bayesian Filter** - enables / disables the pre-trained Bayesian Filter.
- **Enable Multi Filter** - enables / disables the Multi Filter.

  This filter has several components:

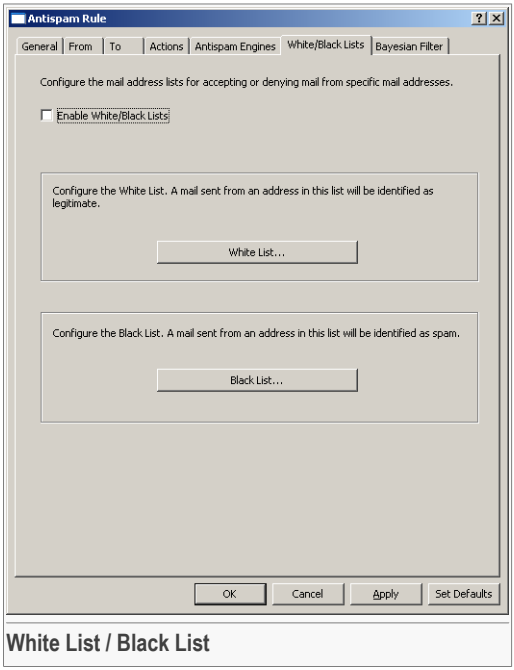
  - **Asian** - enables / disables the filter that blocks mail written in Asian characters.
  - **Cyrillic** - enables / disables the filter that blocks mail written in Cyrillic characters.
  - **Block sexually explicit content** - enables / disables the filter that blocks messages tagged `Sexually-Explicit` in the subject.
- **Enable Image Filter** - enables / disables the Image Filter.

- **Enable URL Filter** - enables / disables the URL Filter.
- **Enable RBL Filter** - enables / disables the global RBL Filter.
- **Enable Heuristic Filter** - enables / disables the Heuristic Filter.

Note
To enable / disable a filter select / clear the corresponding check box.

Step 6/7 - Configure White List / Black List

Click the **White / Black Lists** tab and configure the White List and the Black List.



White List / Black List

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

Check **Enable White / Black Lists** to filter messages using the White List and the Black List.

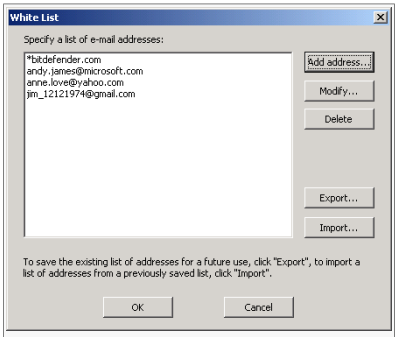
White List

The White List contains e-mail addresses expected to send legitimate messages. Any mail coming from an address contained in the **White list** will be considered legitimate and will bypass further antispam filters.

Note

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

Click **White List** to configure the White List. A new window will appear.



White List

This is where you can see and manage trusted e-mail addresses.

Add Addresses. Click **Add** to add a new address to the list. Provide the address in the window that will appear and then click **OK**.

Manage Addresses. You can see the e-mail addresses listed in the table. If you want to modify an address, either double-click it or select it and click **Modify**. To remove one or several selected addresses, click **Delete** and then **Yes** to confirm your choice.

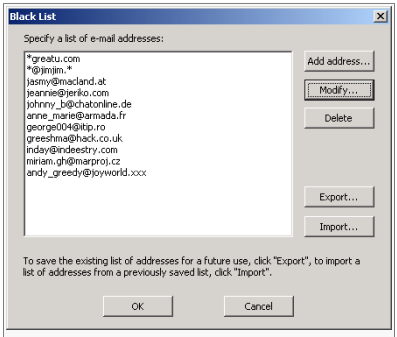
Import / Export Addresses. To import addresses from a `txt` file, click **Import**, select it and then click **Open**. To export the existing addresses to a `txt` file, click **Export** and save the file to the desired location. This way you can use the address list when configuring BitDefender server products on other machines or after reinstalling the product.

Click **OK** to save the changes and close the window. If you click **Cancel** all changes will be lost.

Black List

The Black List contains e-mail addresses expected to send spam messages. Any mail coming from an address contained in the **Black list** will be considered spam and the appropriate action will be taken.

Click **Black List** to configure the Black List. A new window will appear.



Black List

This is where you can see and manage untrusted e-mail addresses.

Add Addresses. Click **Add** to add a new address to the list. Provide the address in the window that will appear and then click **OK**.

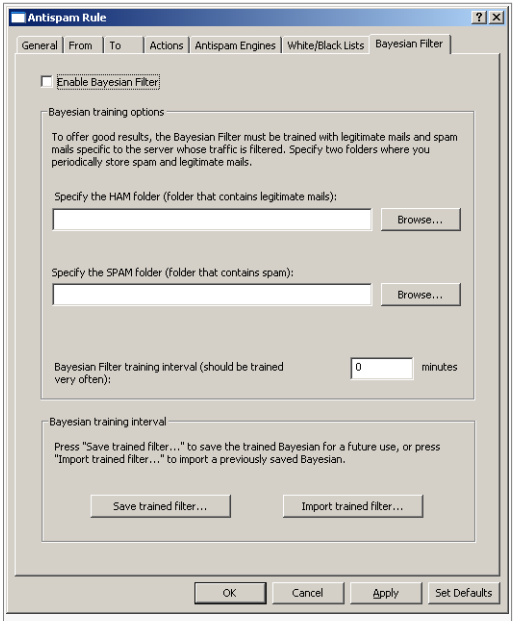
Manage Addresses. You can see the e-mail addresses listed in the table. If you want to modify an address, either double-click it or select it and click **Modify**. To remove one or several selected addresses, click **Delete** and then **Yes** to confirm your choice.

Import / Export Addresses. To import addresses from a `txt` file, click **Import**, select it and then click **Open**. To export the existing addresses to a `txt` file, click **Export** and save the file to the desired location. This way you can use the address list when configuring BitDefender server products on other machines or after reinstalling the product.

Click **OK** to save the changes and close the window. If you click **Cancel** all changes will be lost.

Step 7/7 - Configure Bayesian Filter

Click the **Bayesian Filter** tab and configure the Bayesian Filter.



Bayesian Filter

The Bayesian Filter constantly collects statistical information about server-specific spam and legitimate messages provided by the administrator and it analyzes messages according to this information.

Check **Enable Bayesian Filter** to enable the Bayesian Filter.

To offer good results, the Bayesian Filter must be trained on legitimate messages and spam messages specific to the server whose traffic is filtered. Specify the **HAM folder** (the folder containing legitimate mail) and the **SPAM folder** by clicking **Browse**.

In order to get the best results, it is recommended to train the Bayesian Filter very often. Provide the training interval in the corresponding field.

If you have a previously saved Bayesian Filter, you can import it by clicking **Import trained filter**. To save the current Bayesian Filter for future use, click **Save trained filter**.

Click **OK** to save the changes and close the configuration window.

12. Content Filtering Module

The **Content Filtering** module filters message content based on certain expressions found in the mail headers (subject, from, to, cc).

Based on the groups the sender and the receivers belong to, you can specify various filtering options and actions to be taken on the detected messages.

The module contains two sections:

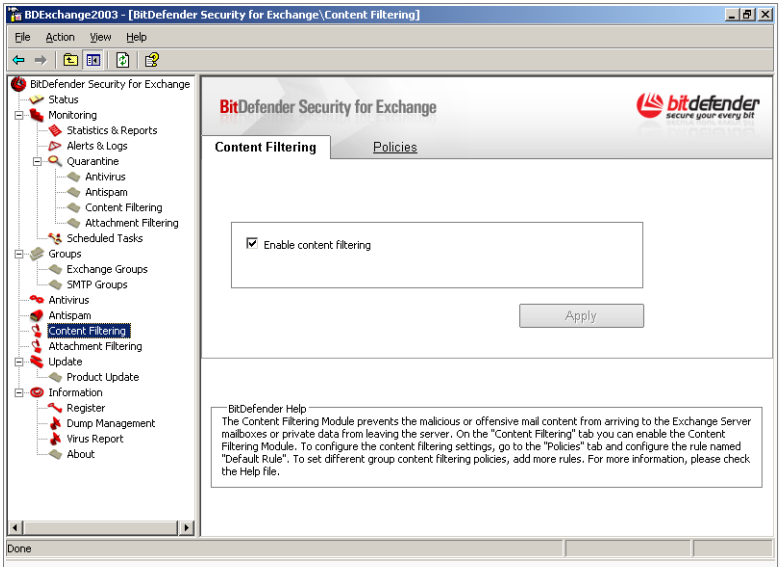
- Content Filtering - allows you to enable the Content Filtering.
- Policies - allows you to configure the filtering options for all incoming mail traffic and to specify different filtering policies based on the groups the sender and the receivers belong to.

Note

Content Filtering is available only for MS Exchange 2000/2003.

12.1. Content Filtering

Click **Content Filtering** in the tree menu to enter this section.



Content Filtering

This is where you can enable content filtering.

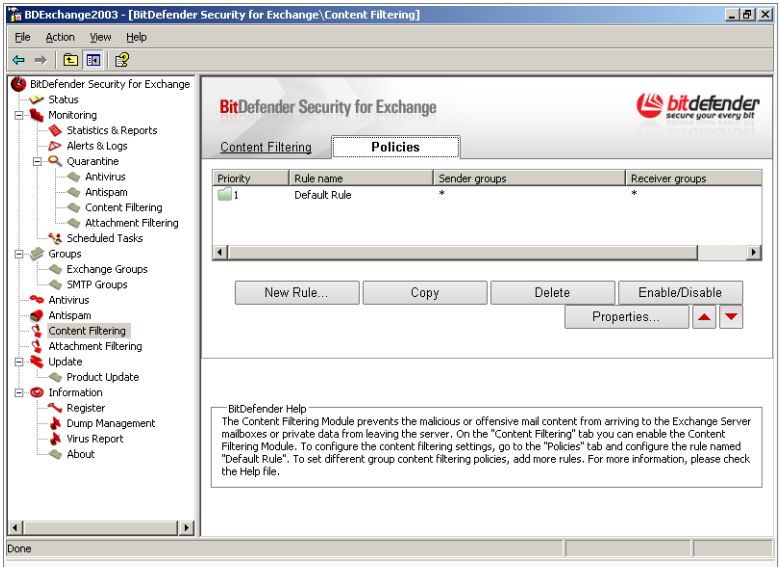
Check **Enable Content Filtering** to enable the content filtering. To disable it, clear the corresponding check box. Click **Apply** to save the changes.

Note

In order to configure the global content filtering options or to create different filtering policies based on user groups, go to the Policies section.

12.2. Setting Policies

Click **Content Filtering** in the tree menu and then the **Policies** tab to enter this section.



Setting Policies

This is where you can specify the content filtering options. You can modify the default rule to specify the content filtering options for all the mail traffic, or you can configure new rules in order to create customized group filtering policies.

12.2.1. Managing Rules

You can see all the existing rules listed in the table. For each rule, the following information is provided: priority, the name and the groups of senders and receivers it applies to. The rules are listed by order of priority with the first rule counting as the highest priority.

Note

Messages are checked against each rule, by order of priority, until the sender and the receivers of the message match a rule. The message is then processed according to the content filtering options specified by that rule.

Default Rule. There is one rule created by default that manages the global content filtering settings. You cannot copy, delete or disable this rule. The default rule has the lowest priority; therefore, you cannot change its priority. Because the rule was designed to apply to the entire mail traffic, you cannot configure group options. However, you can configure all the other options.

Group Filtering Policies. To set different filtering policies, add new rules. This way you can create customized filtering rules for the mail traffic between certain groups of users.

To manage the rules, use the following buttons:

- **New Rule** - creates a new rule. You will have to configure the rule before it appears in the table.
- **Copy** - copies one or several selected rules.
- **Delete** - deletes one or several selected rules. You will have to confirm your choice by clicking **Yes**.
- **Enable / Disable** - enables or disables one or several selected rules.
- **Properties** - opens the configuration window of a selected rule, allowing you to modify the rule. To learn how to configure the rule, please refer to "*Configuring Rules*" (p. 165).
- **Up** - moves a selected rule one level up in the table. This will increase the priority of the rule.
- **Down** - moves a selected rule one level down in the table. This will decrease the priority of the rule.

12.2.2. Creating Rules

To create a rule, choose one of these methods:

- copy an existing rule and click **Properties** to modify it.
- click **New Rule** and configure the new rule.

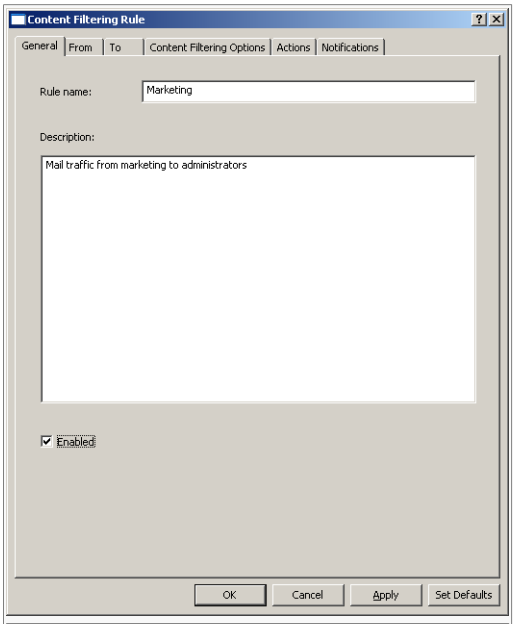
In both cases, a new window will appear. Next, you must configure or modify the rule.

12.2.3. Configuring Rules

To configure a rule follow these steps:

Step 1/6 - Provide General Data

Open the configuration window and provide general data for the rule.



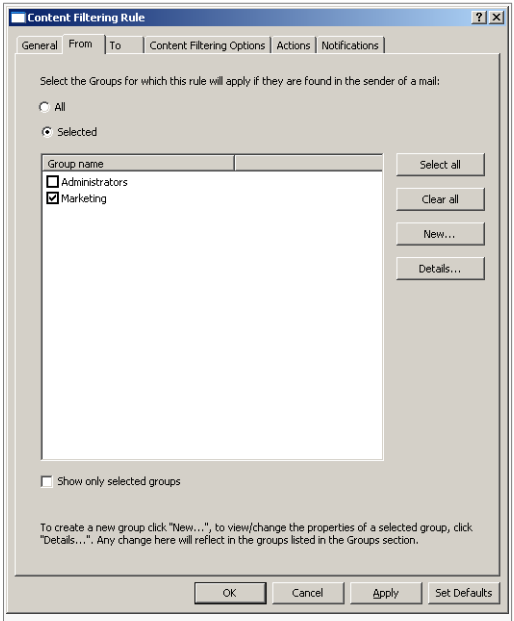
General

Provide the rule name and, optionally, the rule description.

To enable the rule, check **Enabled**. If you want the rule to be disabled, clear the check box.

Step 2/6 - Select Senders Groups

Click the **From** tab and select the groups of senders the rule applies to.



Senders Groups

The following options are available:

- **All** - the rule applies to all senders, no matter if they belong to a group or not.
- **Selected** - the rule applies only to receivers from the selected SMTP groups.

If you choose **Selected**, you have to check from the list the groups you want the rule to apply to.

Click **Select All** to check all groups. If you click **Clear All** no group will be selected.

If necessary, you can create a new SMTP group by clicking **New** and configuring it. The new group will appear in the SMTP Groups section.

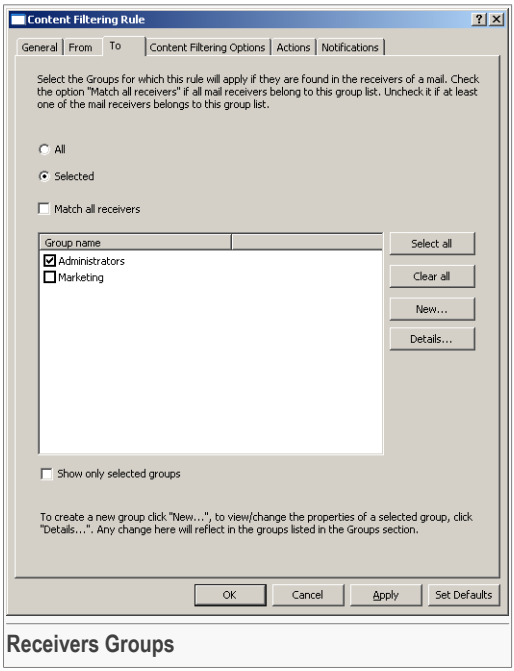
To configure an existing group or to see its parameters, select it and click **Details**.

Note

To learn how to configure an SMTP group, please refer to "*Creating SMTP Groups*" (p. 114).

Step 3/6 - Select Receivers Groups

Click the **To** tab and select the groups of receivers the rule applies to.



Receivers Groups

The following options are available:

- **All** - the rule applies to all receivers, no matter if they belong to a group or not.
- **Selected** - the rule applies only to receivers from the selected SMTP groups.

If you choose **Selected**, you have to check from the list the groups you want the rule to apply to.

You can check the **Match all receivers** option to apply the rule only if all the receivers of the message belong to the specified groups. For example, if the e-mail is sent to

several receivers and at least one of them is not found in the specified groups, the rule will not apply.

Note

The addresses in the **Cc** and **Bcc** fields also count as receivers.

Click **Select All** to check all groups. If you click **Clear All** no group will be selected.

If necessary, you can create a new SMTP group by clicking **New** and configuring it. The new group will appear in the SMTP Groups section.

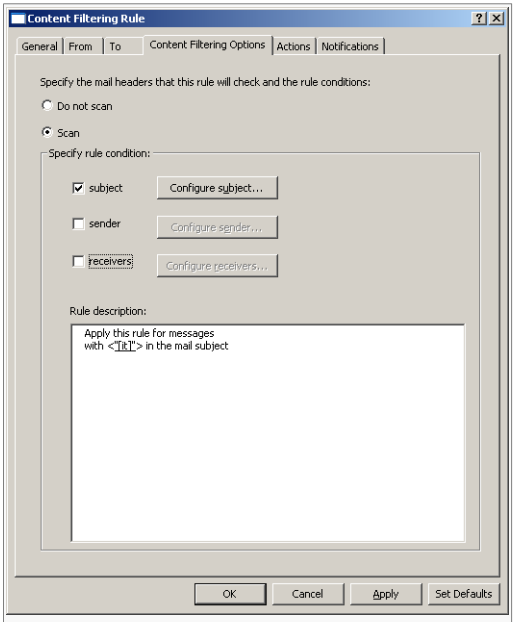
To configure an existing group or to see its parameters, select it and click **Details**.

Note

To learn how to configure an SMTP group, please refer to "*Creating SMTP Groups*" (p. 114).

Step 4/6 - Configure Content Filtering Options

Click the **Content Filtering Options** tab and configure the content filtering options for the messages matching this policy.



Filtering Options

If you do not want to scan the messages using content filtering options, select **Do not scan**. Then, click **OK** to save the changes and close the configuration window.

If you select **Scan**, the messages will be scanned using the content filtering options configured for this policy. Next, you must specify the rule conditions.

Note

Messages that do not match any rule condition will not be detected. Consequently, no action will be taken on them and no notification will be issued.

Messages can be scanned using the following criteria: subject, sender/receiver address. When defining rule conditions, any combination of scanning criteria is allowed.

Filtering Mail by Subject

Check **Subject** and specify the rule strings in order to filter mail by subject. All the messages the subject of which matched one of the defined strings will be detected

To specify the strings, click **Configure subject**. A new window will appear, where you can configure the defined strings (please see "*Configuring Strings*" (p. 170)).

Filtering Mail by Sender Address

Check **Sender** and specify the rule strings in order to filter mail by the sender address. All the messages the sender address of which matches one of the defined strings will be detected

To specify the strings, click **Configure subject**. A new window will appear, where you can configure the defined strings (please see "*Configuring Strings*" (p. 170)).

Filtering Mail by Receiver Address

Check **Receivers** and specify the rule strings in order to filter mail by the receiver address. All messages with at least one receiver address matching one of the defined strings will be detected.

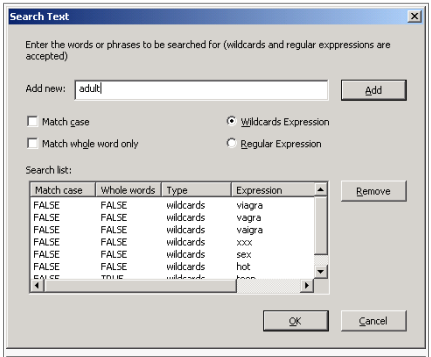
To specify the strings, click **Configure subject**. A new window will appear, where you can configure the defined strings (please see "*Configuring Strings*" (p. 170)).

Configuring Strings

You can see each selected rule condition listed in the box. Click the `specific words` link to specify or modify strings. A configuration window will appear.

Note

To open this window, you can also click **Configure subject**, **Configure sender** or **Configure receivers**.



Specify parameters

Provide the string in the corresponding field and click **Add**.

You can choose to enter either a wildcard expression or a regular expression.

Note

You can use the following wildcards:

- `*` replaces zero, one or more characters.

  For example, you can enter `*xxx*` to detect the messages that contain the `xxx` string in the headers (subject, sender address or receiver address).

- `?` stands for any single character.

  For example, if you filter messages by the sender address, you can `?doe@company.com` to detect the messages that are sent from addresses beginning with any single character and followed by the `doe@company.com` string.

Two additional options are available:

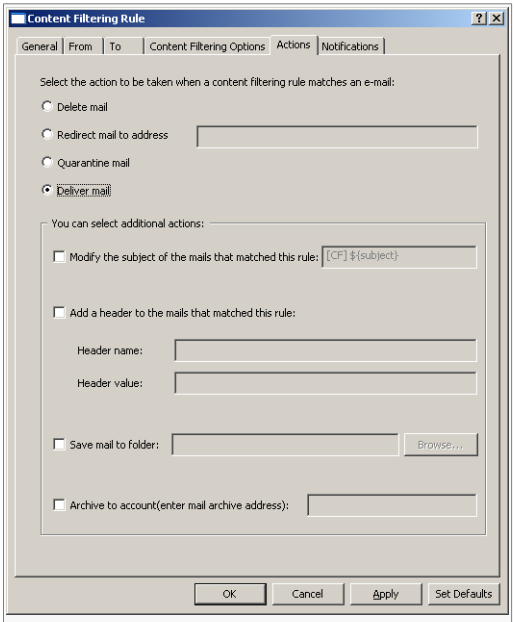
Option	Description
Match case	The rule applies only if the detected item and the specified parameter case match.
Match whole word only	The rule applies only if an entire string matching the specified parameter is detected.

You can see all the defined strings in the list. To remove entries, select them and click **Remove**.

Click **OK** to save the changes.

Step 5/6 - Set Actions

Click the **Actions** tab and specify the actions to be taken on the detected messages.



Actions

You must choose one of the following actions:

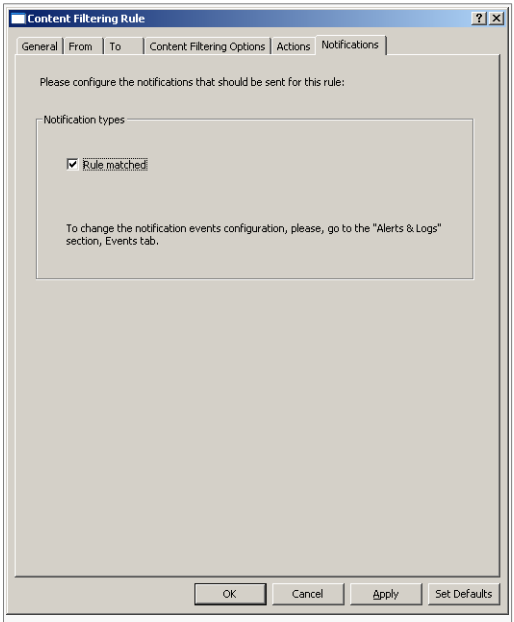
Action	Description
Delete mail	The detected message is deleted.
Redirect mail to address	The detected message is redirected to a specified e-mail address. You must specify the e-mail address where the messages will be delivered in the field next to this option. If you want to provide more than one address, separate them by a semi-colon ";". If the field is empty or the e-mail address is invalid the messages will not be redirected.
Quarantine mail	The detected message is moved to the quarantine folder.
Deliver mail	The detected message is delivered in full to its receivers.

You can also set additional actions to be taken on the detected messages. The following actions are available:

Action	Description
Modify the subject of the mails that matched this rule	The subject of the detected message is modified. You can modify the subject pattern. We recommend you to use one of these patterns: • `[CF]${subject}` - to add `[CF]` before the subject. This is the default subject pattern. • `[CF]${subject}[CF]` - to add `[CF]` before and after the subject. • `[CF]` - to replace the subject with `[CF]`.
Add a header to the mails that matched this rule	An e-mail header is added to the detected message. Provide the header name and value in the corresponding fields.
Save mail to folder	The detected message is saved to a specified folder. To specify the folder, click **Browse**, locate it and then click **OK**.
Archive to account	The detected message is archived to a specified account. Provide the e-mail archive address in the field next to this option. A Bcc containing the address will be added to the detected message.

Step 6/6 - Configure Notifications

Click the **Notifications** tab and specify whether to issue notifications or not when messages match the rule.



Notifications

Check **Rule matched** to issue notifications when messages match the rule.

Note

The corresponding event in the Events section must be enabled and properly configured. For more information, please refer to "*Configuring Events*" (p. 57).

Click **OK** to save the changes and close the configuration window.

13. Attachment Filtering Module

The **Attachment Filtering** module provides filtering features for mail attachments. It can detect attachments with certain name patterns, of a certain type or exceeding a certain size limit.

Based on the groups the sender and the receivers belong to, you can specify various filtering options and actions to be taken on the detected attachments.

The module contains two sections:

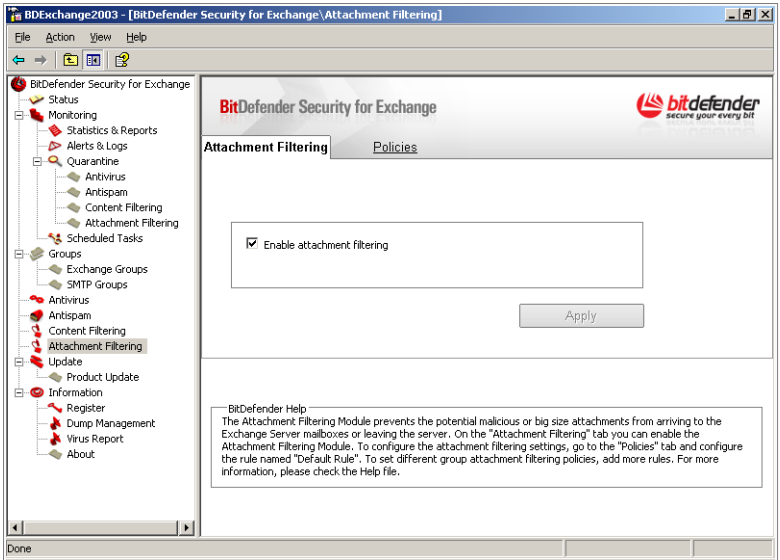
- Attachment Filtering - allows you to enable the Attachment Filtering.
- Policies - allows you to configure the filtering options for all incoming mail traffic and to specify different filtering policies based on the groups the sender and the receivers belong to.

Note

Attachment Filtering is available only for MS Exchange 2000/2003.

13.1. Attachment Filtering

Click **Attachment Filtering** in the tree menu to enter this section.



Attachment Filtering

This is where you can enable attachment filtering.

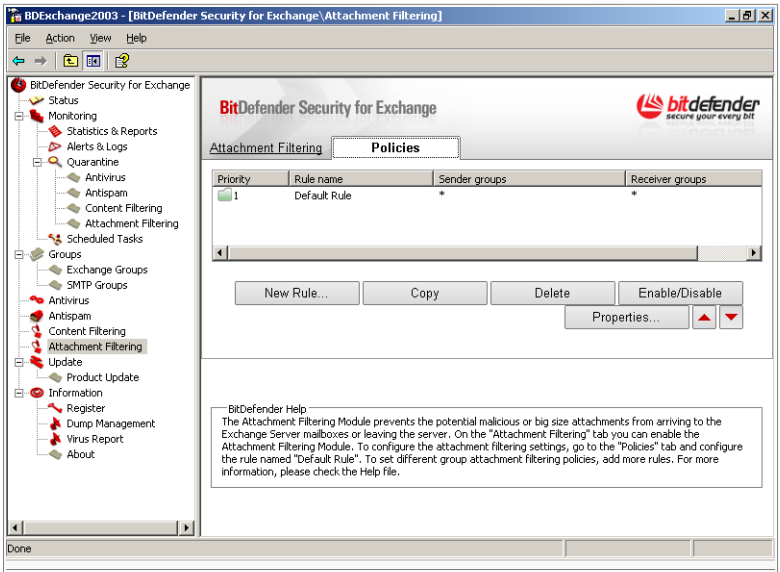
Check **Enable Attachment Filtering** to enable attachment filtering. To disable it, clear the corresponding check box. Click **Apply** to save the changes.

Note

In order to configure the global attachment filtering options or to create different filtering policies based on user groups, go to the Policies section.

13.2. Setting Policies

Click **Attachment Filtering** in the tree menu and then the **Policies** tab to enter this section.



Setting Policies

This is where you can specify the attachment filtering options. You can modify the default rule to specify the attachment filtering options for all the mail traffic, or you can configure new rules in order to create customized group filtering policies.

13.2.1. Managing Rules

You can see all the existing rules listed in the table. For each rule, the following information is provided: priority, the name and the groups of senders and receivers it applies to. The rules are listed by order of priority with the first rule counting as the highest priority.

Note

Messages are checked against each rule, by order of priority, until the sender and the receivers of the message match a rule. The message is then processed according to the attachment filtering options specified by that rule.

Default Rule. There is one rule created by default that manages the global content filtering settings. You cannot copy, delete or disable this rule. The default rule has the lowest priority; therefore, you cannot change its priority. Because the rule was designed to apply to the entire mail traffic, you cannot configure group options. However, you can configure all the other options.

Group Filtering Policies. To set different filtering policies, add new rules. This way you can create customized filtering rules for the mail traffic between certain groups of users.

To manage the rules, use the following buttons:

- **New Rule** - creates a new rule. You will have to configure the rule before it appears in the table.
- **Copy** - copies one or several selected rules.
- **Delete** - deletes one or several selected rules. You will have to confirm your choice by clicking **Yes**.
- **Enable / Disable** - enables or disables one or several selected rules.
- **Properties** - opens the configuration window of a selected rule, allowing you to modify the rule. To learn how to configure the rule, please refer to "*Configuring Rules*" (p. 179).
- **Up** - moves a selected rule one level up in the table. This will increase the priority of the rule.
- **Down** - moves a selected rule one level down in the table. This will decrease the priority of the rule.

13.2.2. Creating Rules

To create a rule, choose one of these methods:

- copy an existing rule and click **Properties** to modify it.
- click **New Rule** and configure the new rule.

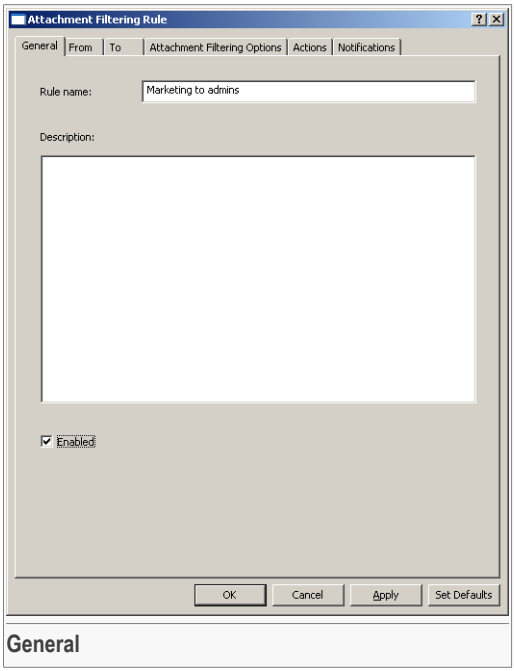
In both cases, a new window will appear. Next, you must configure or modify the rule.

13.2.3. Configuring Rules

To configure a rule follow these steps:

Step 1/6 - Provide General Data

Open the configuration window and provide general data for the rule.



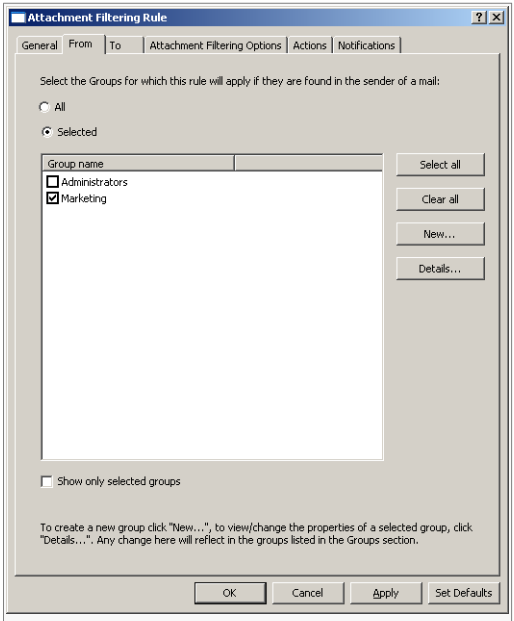
General

Provide the rule name and, optionally, the rule description.

To enable the rule, check **Enabled**. If you want the rule to be disabled, clear the check box.

Step 2/6 - Select Senders Groups

Click the **From** tab and select the groups of senders the rule applies to.



Senders Groups

The following options are available:

- **All** - the rule applies to all senders, no matter if they belong to a group or not.
- **Selected** - the rule applies only to receivers from the selected SMTP groups.

If you choose **Selected**, you have to check from the list the groups you want the rule to apply to.

Click **Select All** to check all groups. If you click **Clear All** no group will be selected.

If necessary, you can create a new SMTP group by clicking **New** and configuring it. The new group will appear in the SMTP Groups section.

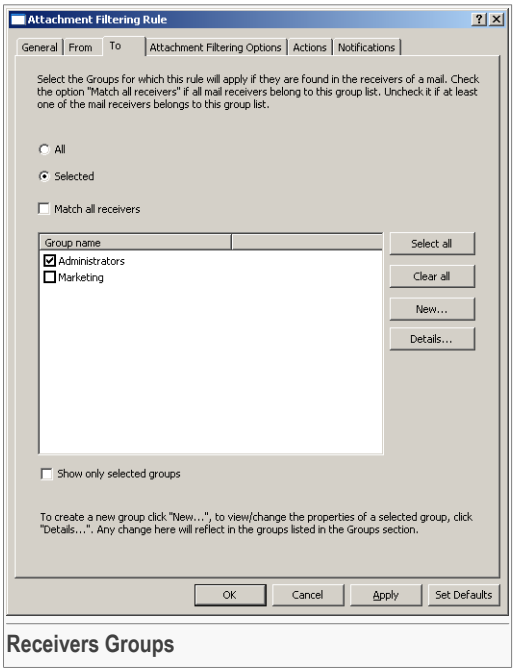
To configure an existing group or to see its parameters, select it and click **Details**.

Note

To learn how to configure an SMTP group, please refer to "*Creating SMTP Groups*" (p. 114).

Step 3/6 - Select Receivers Groups

Click the **To** tab and select the groups of receivers the rule applies to.



Receivers Groups

The following options are available:

- **All** - the rule applies to all receivers, no matter if they belong to a group or not.
- **Selected** - the rule applies only to receivers from the selected SMTP groups.

If you choose **Selected**, you have to check from the list the groups you want the rule to apply to.

You can check the **Match all receivers** option to apply the rule only if all the receivers of the message belong to the specified groups. For example, if the e-mail is sent to

several receivers and at least one of them is not found in the specified groups, the rule will not apply.

Note

The addresses in the **Cc** and **Bcc** fields also count as receivers.

Click **Select All** to check all groups. If you click **Clear All** no group will be selected.

If necessary, you can create a new SMTP group by clicking **New** and configuring it. The new group will appear in the SMTP Groups section.

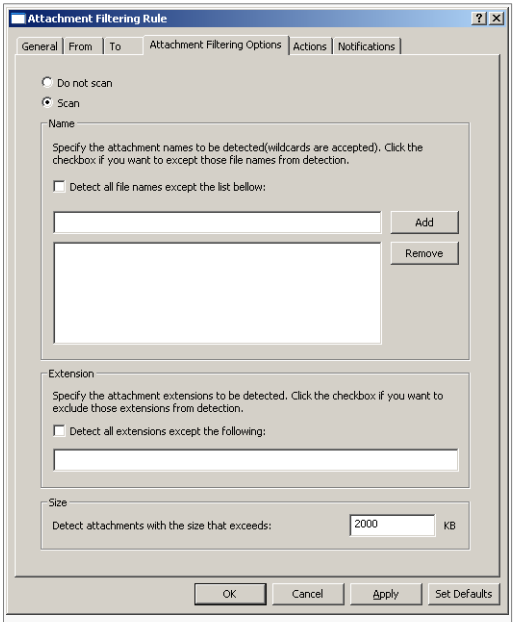
To configure an existing group or to see its parameters, select it and click **Details**.

Note

To learn how to configure an SMTP group, please refer to "*Creating SMTP Groups*" (p. 114).

Step 4/6 - Configure Attachment Filtering Options

Click the **Attachment Filtering Options** tab and configure the filtering options for the messages matching this policy.



Filtering Options

If you do not want to scan the messages using attachment filtering options, select **Do not scan**. Then, click **OK** to save the changes and close the configuration window.

If you select **Scan**, the messages will be scanned using the attachment filtering options configured for this policy. Next, you must specify the rule conditions.

Note

Messages that do not match any rule condition will not be detected. Consequently, no action will be taken on them and no notification will be issued.

Mail attachments can be scanned using the following criteria: name, file extension and file size. When defining rule conditions, any combination of scanning criteria is allowed.

Filtering Attachments by Name

Check **Detect all filenames except the list below** and specify the excepted filenames in order to filter attachments by name. All attachments with filenames other than those specified as exceptions will be detected.

Note

The term `name` refers here to the filename and the filename extension. For example, if the filename is `name_of_file` and the filename extension is `ext`, then the name you have to specify as exception is `name_of_file.ext`.

To specify exceptions, provide the name in the edit field and click **Add**.

Note

Wildcards can be used to specify exceptions:

- `*` replaces zero, one or more characters.

  For example, you can enter `file*.exe` to specify a large category of filenames, which includes filenames like `file01.exe`, `file_new.exe`, `file.exe` and others.

- `?` stands for any single character.

  For example, you can enter `group?_log??.doc` to specify a large category of filenames, which includes filenames like `group1_log01.doc`, `groupA_log19.doc`, `group4_log1a.doc` and others.

All the names excepted from scanning are listed in the box. To remove entries, select them and click **Remove**.

Filtering Attachments by Type

Check **Detect all extensions except the list below** and specify the excepted extensions in order to filter attachments by type. All attachments with extensions other than those specified as exceptions will be detected.

Specify the permitted extensions in the edit field. The extensions must be separated by a semi-colon ";".

Note

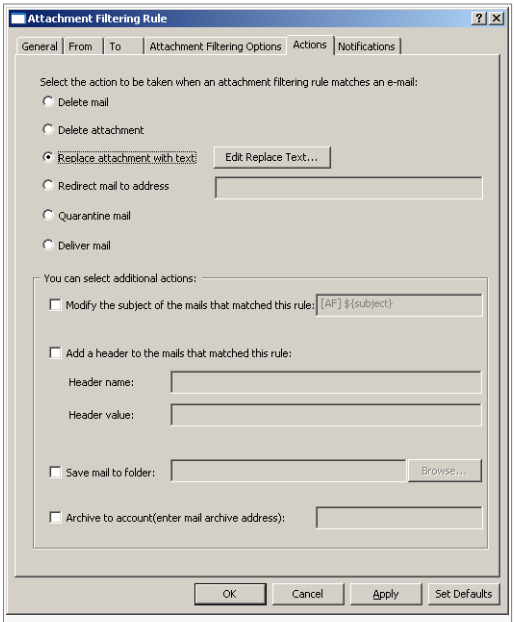
In case of a double extension, only the last extension will be checked.

Filtering Attachments by Size

To detect attachments exceeding a certain size limit, specify the minimum size in the corresponding field. By default, this is set to 0 KB, meaning that no attachment will be detected regardless of its size.

Step 5/6 - Set Actions

Click the **Actions** tab and specify the actions to be taken on the messages containing detected attachments.



Actions

You must choose one of the following actions:

Action	Description
Delete mail	The message containing the detected attachment is deleted.
Delete attachment	The detected attachment is deleted.
Replace attachment with text	The detected attachment is replaced with a specified text. To specify the text to be delivered instead of the attachment, click **Edit Replace Text**. Provide the text in the edit box that appears and click **OK**.

Action	Description
Redirect mail to address	The message containing the detected attachment is redirected to a specified e-mail address. You must specify the e-mail address where the messages will be delivered in the field next to this option. If you want to provide more than one address, separate them by a semi-colon ";". If the field is empty or the e-mail address is invalid the messages will not be redirected.
Quarantine mail	The message containing the detected attachment is moved to the quarantine folder.
Deliver mail	The message containing the detected attachment is delivered in full to its receivers.

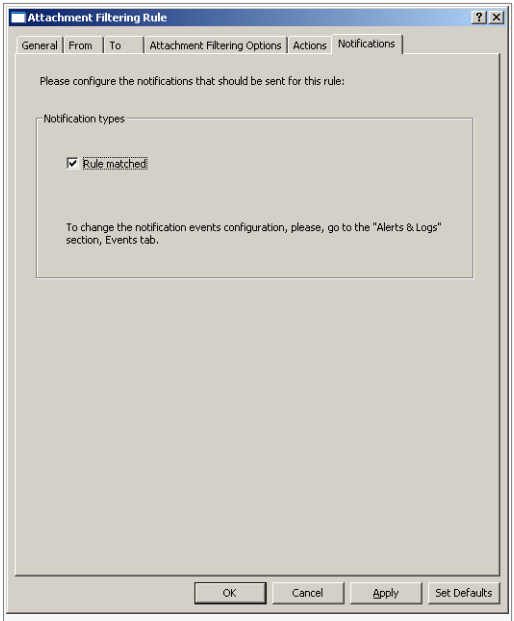
You can also set additional actions to be taken on the detected messages. The following actions are available:

Action	Description
Modify the subject of the mails that matched this rule	The subject of the message containing the detected attachments is modified. You can modify the subject pattern. We recommend you to use one of these patterns: • `[AF]${subject}` - to add `[AF]` before the subject. This is the default subject pattern. • `[AF]${subject}[AF]` - to add `[AF]` before and after the subject. • `[AF]` - to replace the subject with `[AF]`.
Add a header to the mails that matched this rule	An e-mail header is added to the message containing the detected attachment. Provide the header name and value in the corresponding fields.
Save mail to folder	The detected message is saved to a specified folder.

Action	Description
	To specify the folder, click **Browse**, locate it and then click **OK**.
Archive to account	The detected message is archived to a specified account. Provide the e-mail archive address in the field next to this option. A Bcc containing the address will be added to the detected message.

Step 6/6 - Configure Notifications

Click the **Notifications** tab and specify whether to issue notifications or not when attachments match the rule.



Notifications

Check **Rule matched** to issue notifications when attachments match the rule.

Note

The corresponding event in the Events section must be enabled and properly configured. For more information, please refer to "*Configuring Events*" (p. 57).

Click **OK** to save the changes and close the configuration window.

14. Update Module

New viruses and spyware are found and identified every day. This is why it is very important to keep BitDefender up to date with the latest signatures. By default, BitDefender automatically checks for updates every hour.

Updates come in the following ways:

- **Updates for the antivirus engines** - the files containing virus and spyware signatures are updated to ensure permanent up-to-date protection against them. This update type is also known as **Virus Definitions Update**.
- **Updates for the antispam engines** - new rules are added to the NeuNet (heuristic) and Pre-trained Bayesian filters, new links are added to the URL filter database and new images are added to the Image filter; this will help increase the effectiveness of your Antispam engine. This update type is also known as **Antispam Update**.
- Product updates - 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**.

Moreover, from the user's intervention viewpoint, we may take into account:

- Automatic update - BitDefender automatically contacts the update server in order to check if an update was released. If there are available updates, BitDefender is updated automatically.

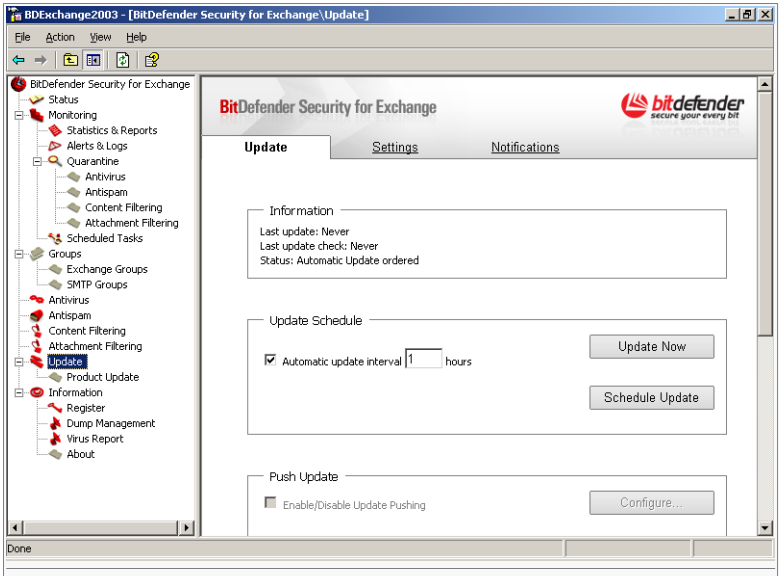
  Note

  In order not to interfere with the server's operation, product updates are not automatically installed. Go to the Product Update section periodically to see if there are any product updates available and to install them.

  The automatic update can also be done anytime you want by clicking **Update now** from the Update module or by creating a scheduled update task.
- Manual update - you must download and install the latest virus and spyware definitions manually.

14.1. Automatic Update

Click **Update** in the tree menu to enter this section.



Automatic Update

This is where you can see update-related information and perform updates.

In the **Information** box, you can see the update status and when the last update check and update were performed.

14.1.1. Updating BitDefender

There are 4 ways to update BitDefender:

- **Automatically.** By default, BitDefender checks for updates at the specified update locations on a regular basis. The default time interval is one hour. To change this interval, provide a new value in the edit field. If an update is detected, BitDefender will automatically download and install the new signatures, without the administrator's intervention.

Important

Keep the automatic update enabled in order to be protected against the latest threats.

To disable automatic update, clear the check box corresponding to **Automatic update interval** and click **Apply**.

- **By user request.** Just click the **Update Now** button when you want to update BitDefender. The Update module will connect to the BitDefender update server and it will check if any update is available. If an update is detected, BitDefender will automatically download and install the new signatures.
- **Using a scheduled task.** Click **Schedule Update** to schedule an update task. For more details, check "*Update Tasks*" (p. 69).

Note

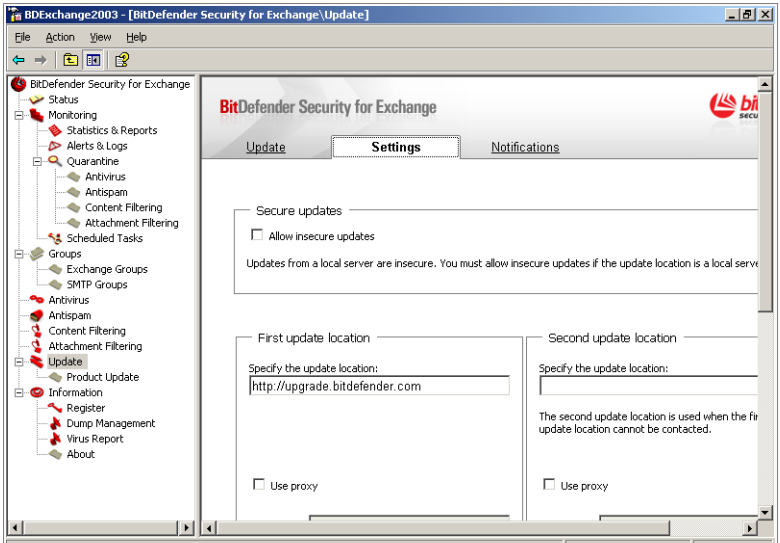
The scheduled update tasks will not deactivate the automatic update module, which will check the update server for new signatures on a regular basis.

- **Through Update Pushing.** The Update Pushing is a feature that is available only when the product is registered. This feature allows customers to benefit from "Update Announcement Messages". These alerts are sent to the Update Pushing mailing list by the BitDefender Lab. The mailing list is composed of mail addresses that have been submitted by the customers on the BitDefender website. The "Update Announcement Messages" include special elements which trigger the update process when the message is scanned by the product. Therefore, it is mandatory that the mail address submitted by the customer is a mail address protected by BitDefender. To enable Update Pushing, check **Enable/Disable Update Pushing**. If you do not want to use this service, clear the corresponding check box. To subscribe to the mailing list, click **Configure**.

Click **Apply** to save the changes.

14.2. Update Settings

Click **Update** in the tree menu and then the **Settings** tab to enter this section.



Update Settings

This is where you can configure the update locations.

The updates can be performed from the local network, over the Internet, directly or through a proxy server.

14.2.1. Local Updates

Updates placed on a local server are not secure. Unlike the updates downloaded from the BitDefender servers, local updates are not signed.

To allow updates from a local server to be installed, check **Allow insecure updates**.

Local update mirrors also pose another risk. Suppose BitDefender is usually updated daily from an official location and, for some reason, this location is not available for a new update at a certain moment. If you have set a local server as the second update location, then BitDefender will download and use the signatures available in this location. If the local server is not synchronized with the BitDefender server, there is

the risk that the installed signatures are older than those used by BitDefender before the update. In this way, instead of being upgraded, BitDefender can be downgraded.

14.2.2. Setting Update Locations

For more reliable and faster updates, you can configure two update locations: a **First update location** and a **Second update location**. Both require the configuration of the following options:

- **Update location** - type the address of the update server. By default, the primary update location is: `upgrade.bitdefender.com`.

  Note

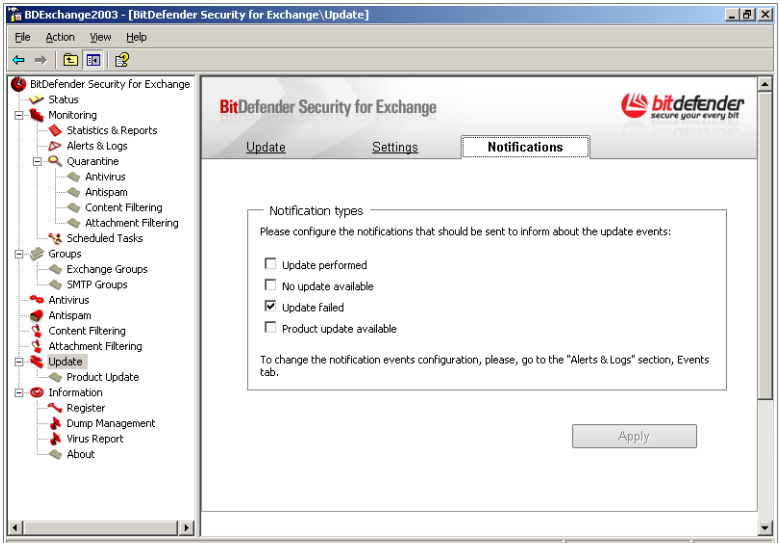
  If you are connected to a local network that has BitDefender virus signatures placed locally, you can change the location of the updates here.

- **Use proxy** - check this option if the company uses a proxy server. The following settings must be specified:
  - **Server IP** - type the IP of the proxy server.
  - **Port** - type the port BitDefender uses to connect to the proxy server.
  - **User name** - type a user name recognized by the proxy.
  - **Password** - type the valid password of the previously specified user.

Click **Apply** to save the changes.

14.3. Update Notifications

Click **Update** in the tree menu and then the **Notifications** tab to enter this section.



Update Notifications

This is where you can specify the update events for which notifications should be issued.

Check the update events for which to issue notifications:

- **Update performed** - when an update was performed.
- **No update available** - when no update is available.
- **Update failed** - when an error occurred during an update and the update failed.
- **Product update available** - when a product update is available.

Note

The corresponding events from the Events section must be enabled and properly configured. For more information, please refer to "*Configuring Events*" (p. 57).

Click **Apply** to save the changes.

14.4. Manual Update

This method allows installing the latest virus and spyware signatures. To install a patch or a product upgrade of the latest version, go to the Product Update section.

Important

Use the manual update when the automatic update can not be performed or when the computer is not connected to the Internet.

Manual update is performed using zip archives. There are two zip archives on the update server, containing the updates of the scanning engines and virus and spyware signatures: `cumulative.zip` and `daily.zip`.

- `cumulative.zip` is released every week on Monday and it includes all the virus and spyware definitions and scan engines updates up to the release date.

Note

The download locations, on FTP and HTTP, are:

- ftp://ftp.bitdefender.com/pub/updates/update_is_90/cumulative.zip
- http://download.bitdefender.com/updates/update_is_90/cumulative.zip

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

Note

The download locations, on FTP and HTTP, are:

- ftp://ftp.bitdefender.com/pub/updates/update_is_90/daily.zip
- http://download.bitdefender.com/update_is_90/daily.zip

Steps to be followed:

1. **Download the update files.** If it is Monday, please download the cumulative.zip and save it somewhere on your disk when prompted. Otherwise, please download the daily.zip and save it on your disk. If this is the first time you update using the manual updates, please download the both archives.
2. **Stop antivirus protection.** Open the management console, click **Antivirus** in the tree menu and clear the check box next to **Enable real time antivirus scanning**.
3. **Open Services.** Follow the path: **Start** → **Control Panel** → **Administrative Tools** → **Services**.

4. **Stop BitDefender Scanning Service.** Right-click BitDefender Scanning Service (BDSCAND) and select **Stop**.
5. **Stop BitDefender File Service.** Right-click BitDefender File Service (BDFILED) and select **Stop**.
6. **Stop BDConnector Service.** Right-click BDConnector Service (bdconnector) and select **Stop**.
7. **Copy the update files.** Extract the content of the archive in the `?:\Program Files\Common Files\Softwin\AV\Plugins` folder and accept overwriting existing files.

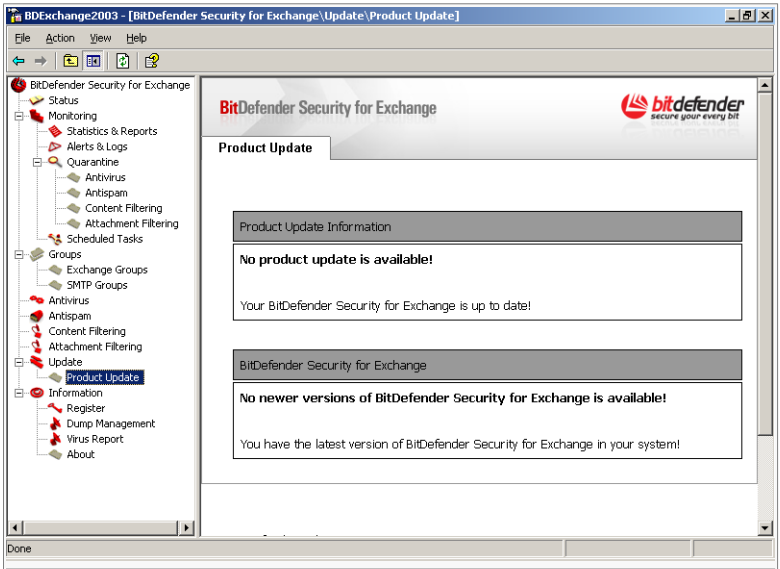
Note

Start with `cumulative.zip` when both update archives are available.

8. **Start BitDefender Scanning Service.** Right-click BitDefender Scanning Service (BDSCAND) and select **Start**.
9. **Start BitDefender File Service.** Right-click BitDefender File Service (BDFILED) and select **Start**.
10. **Start BitDefender BDConnector Service.** Right-click BDConnector Service (bdconnector) and select **Start**.
11. **Start antivirus protection.** Open the management console, click **Antivirus** in the tree menu and check **Enable real time antivirus scanning**.

14.5. Product Update

Click **Product Update** in the tree menu (**Update** module) to enter this section.



Product Update

This is where you can see if product updates or newer product versions are available and install them, if any.

The product updates are different from the signature updates. Their function is to deliver bug fixes and performance improvements of the product.

There are two types of updates for the product:

- **product updates (patches)** - these are cumulative `.exe` files that include all the files that have been changed since the first release of a specific version.
- **version updates** - these are installation packages of a new released version of the product.

Note

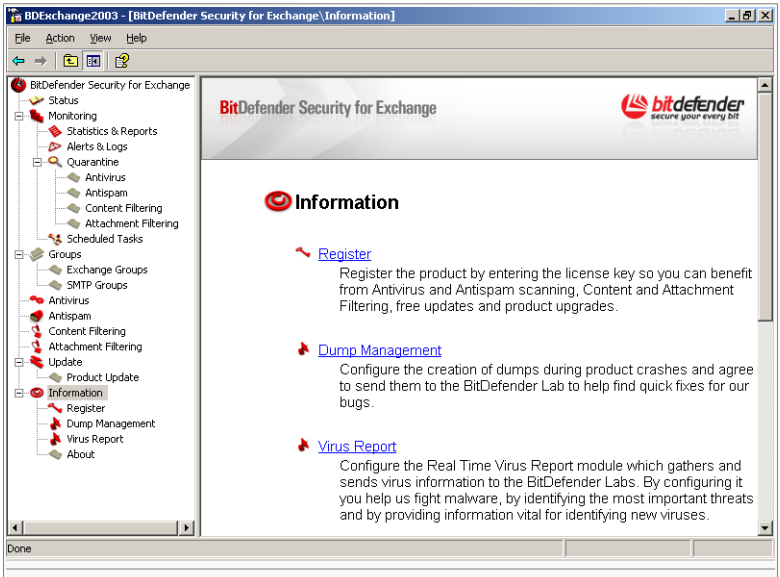
Patches and newer product versions are not automatically installed because they might require a system restart. We advise you to install the latest version of product updates or product version.

When a new patch is available, it is downloaded on the local computer and information about it is displayed. Also, a link to the web page containing the patch description is provided. Click **Install** to install the patch.

When a newer version of BitDefender Security for Exchange is available, you will see information about that version. Also, you will be provided with a link to the web page where you can download the installation package from. Click the respective link and download and install the new version.

15. Information Module

Click **Information** in the tree menu to access this section.



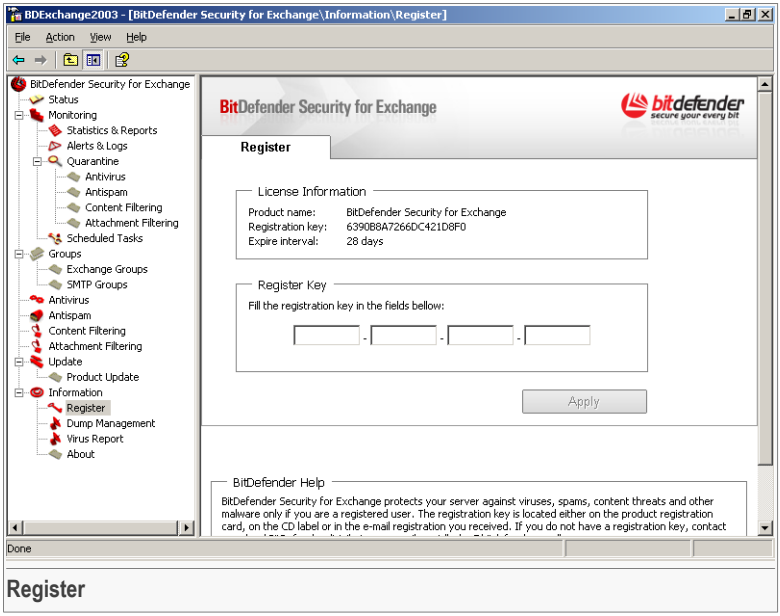
Information

The **Information** module contains the following sections:

- Register - this is where you can register the product
- Dump Management - this is where you can agree to send us dumps created during product crashes.
- Virus Report - this is where configure the Real-time Virus Reporting.
- About - this is where you can view the BitDefender modules installed and their corresponding versions.

15.1. Product Registration

Click **Register** in the tree menu (**Information** module) to enter this section.



Register

This is where you can register the product and see the license information.

The product is delivered with a trial license key valid for thirty days.

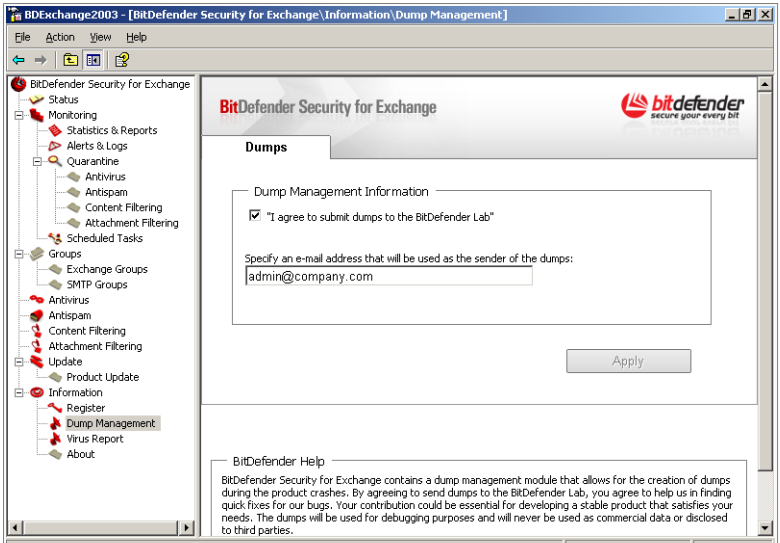
To change the license key, type the new one in the corresponding fields and click **Apply**. The expiration date of the new license key will appear in the **Expire interval** field.

Note

You can find the registration key either on the product registration card, on the CD label or in the registration e-mail you received. If you do not have a registration key, contact your local BitDefender distributor or e-mail us at <sales@bitdefender.com>.

15.2. Dump Management

Click **Dump Management** in the tree menu (**Information** module) to enter this section.



Dump Management

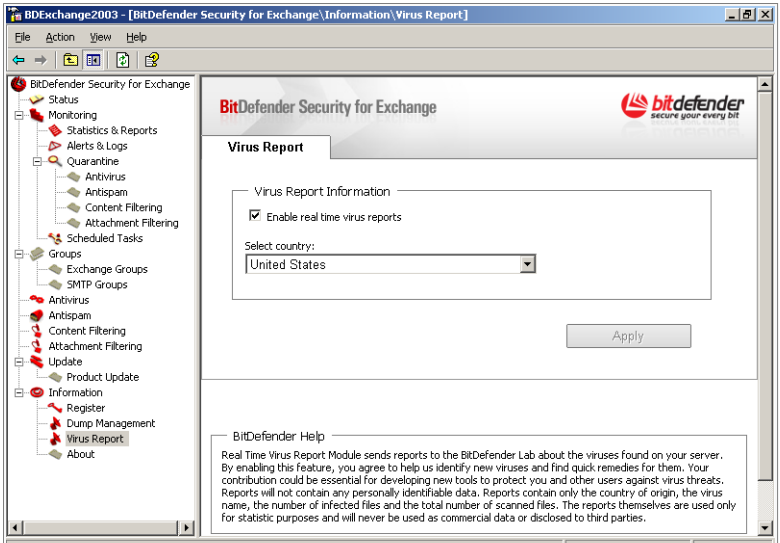
BitDefender Security for Exchange contains a dump management module that allows for the creation of dumps during product crashes. By agreeing to send the dumps to the BitDefender Lab, you agree to help us in finding quick fixes for our bugs. Your contribution could be essential for developing a stable product that satisfies your needs. The dumps will be used for debugging purposes and will never be used as commercial data or disclosed to the third parties.

To send dumps to the BitDefender Lab, check **I agree to submit dumps to the BitDefender Lab** and specify your e-mail address.

Click **Apply** to save changes.

15.3. Real-time Virus Reporting

Click **Virus Report** in the tree menu (**Information** module) to enter this section.



Real-time Virus Reporting

Real-time Virus Reporting (RTVR) allows sending reports about the viruses found on your server to the BitDefender Lab in order to help us identify new viruses and find quick remedies for them. Your contribution could be essential for developing new tools to protect you and other users against virus threats.

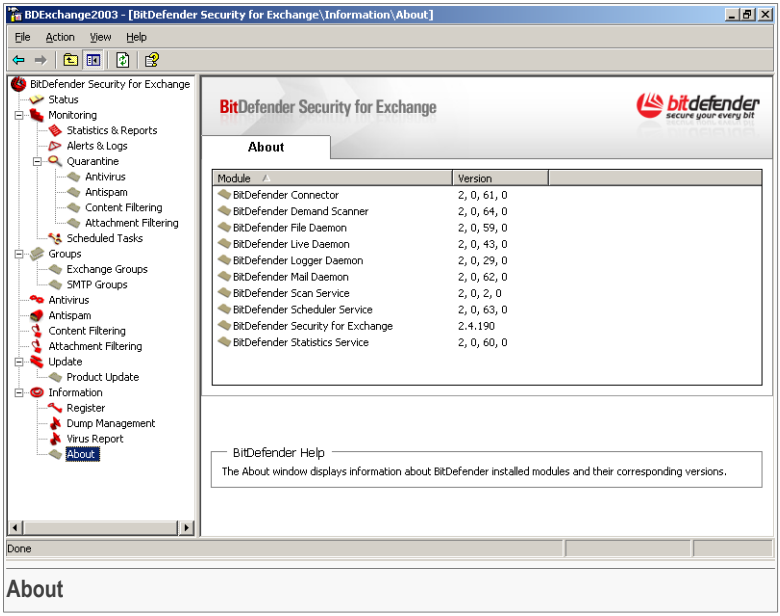
The reports will not contain any personally identifiable data, such as your name, IP address or others. The information supplied will contain only the name of the country, the virus name, the number of infected files and the total number of scanned files. The reports themselves are used only for statistic purposes and will never be used as commercial data or disclosed to third parties.

To activate Real-time Virus Reporting, check **Enable real time virus reports** and then select the country where you live in from the list. If you want to disable it, clear the corresponding check box.

Click **Apply** to save the changes.

15.4. About

Click **About** in the tree menu (**Information** module) to enter this section.



This is where you can see all the BitDefender installed components and their corresponding versions.

BitDefender Enterprise Manager Integration

16. BitDefender Enterprise Manager

BitDefender Enterprise Manager allows for the full automation of routine tasks (including upgrades and updates), while enabling the administrator to 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), which can be executed across the BitDefender Enterprise Manager network. The WMI server add-on is available with BitDefender Enterprise Manager v2.5.

BitDefender Enterprise Manager has been 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.

16.1. The Top Solution for Complex Networks Security

- 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
- Use WMI controls to stop potentially harmful tasks from running on workstations
- 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

16.2. Key Features

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

computer running Windows NT4.0/2000/XP/2003 will do. A wizard is available to guide you through the installation process. BitDefender Enterprise Manager allows for a centralized multi-platform integrated installation.

All in One Installation Kit. Starting with Enterprise Manager 2.6 there is a single installation kit containing all components. Now, you can install not only one server add-on at a time, but all together in one single installation process. There is no need to first install the BitDefender Local Manager and after that to install a particular server add-on. At present, a server add-on already contains the BDLM.

Remote Management. The BitDefender Enterprise Management Console can be installed anywhere in the network. The Console can perform remote server configuration and client management. Management is available from any network connected system, drastically reducing incident response time.

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, deploy them throughout the network, start scan processes at different preset network levels, delete or repair suspicious or infected files and 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.

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 immediately spot which stations needs their attention.

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

Modular Structure. The product modular design makes it easily adaptable to any working environment.

24/7 Professional Technical Support. Qualified support representatives and an online database are available to our customers at no extra cost.

17. Why BitDefender Enterprise Manager?

BitDefender Enterprise Manager is a scalable, superior solution for the centralized management of antivirus protection in complex networks. It combines both the advantages of defining and controlling network security policies, and the 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.

17.1. BitDefender Enterprise Manager Integration Advantages

BitDefender Security for Exchange deeply integrates with BitDefender Enterprise Manager, which allows configuring and monitoring the former from the Enterprise Management Console.

The additional BitDefender Security for Exchange task templates from the BitDefender Enterprise Manager interface offer several benefits and advantages:

Configure BitDefender Security for Exchange.

- Allows for the configuration of all BitDefender Security for Exchange settings in a single step.
- Ensures a uniform BitDefender configuration, according to the pre-established internal policy, by running the task on all BitDefender Security for Exchange clients.
- Offers the possibility of passing the product management task from the local admin of the server on to a security products admin.
- Does not require any additional rights when remotely configuring BitDefender Security for Exchange. Consequently, no modification of the internal right policy is necessary.

Get BitDefender Security for Exchange Statistics.

- Offers general or specific information about the activity of a BitDefender Security for Exchange client, in a selected time interval. By running the task one time only, it is possible to acquire information about one or more clients.

- Monitors the activity of a single client or of all BitDefender Security for Exchange clients, by generating reports based on the results of this task. The reports can be generated periodically, printed or exported in HTML format for further information processing.
- Provides an overview of the global protection of all of the products in the organization.
- Offers the possibility of passing the server security monitoring task from the local admin of the server on to a security products admin.

Get Servers Status.

- Offers a list of the entire configuration of a BitDefender Security for Exchange client, which is to be found in the **Active Tasks** section. By running the task one-time only, it is possible to acquire information about one or more clients.
- Offers centralized information on all BitDefender Security for Exchange clients, by generating reports based on the results of this task. The reports can be generated periodically, printed or exported in HTML format for further information processing.

Scan Exchange Files (BitDefender Security for Exchange).

- Allows scanning the files of Exchange servers on which BitDefender Security for Exchange clients are installed.
- Ensures additional security and low impact on server activity, by running the task on all BitDefender Security for Exchange clients during low activity periods, according to a pre-established internal policy.
- Offers the possibility of passing this security task from the local admin of the server on to a security products admin.

Update Servers.

- Allows centralized update management for all BitDefender Security for Exchange clients.
- Keeps BitDefender clients up-to-date, by running the task periodically on all BitDefender Security for Exchange clients, according to a pre-established policy.
- Ensures low impact on server activity, by updating all BitDefender Security for Exchange clients during low activity periods.
- Offers the possibility of passing the product updating task from the local admin of the server on to a security products admin.

18. Additional Task Templates

BitDefender Security for Exchange deeply integrates with BitDefender Enterprise Manager, which allows configuring and monitoring the former from the Enterprise Management Console

Note

BitDefender Security for Exchange must be installed on a BitDefender Enterprise Manager client. This is due to the fact that **BitDefender Local Manager** must already be installed on a workstation in order to be able to import the tasks from the BitDefender products installed on that workstation.

To open the Enterprise Management Console follow this path: **Start** → **Programs** → **BitDefender Enterprise Manager** → **BitDefender Management Console**.

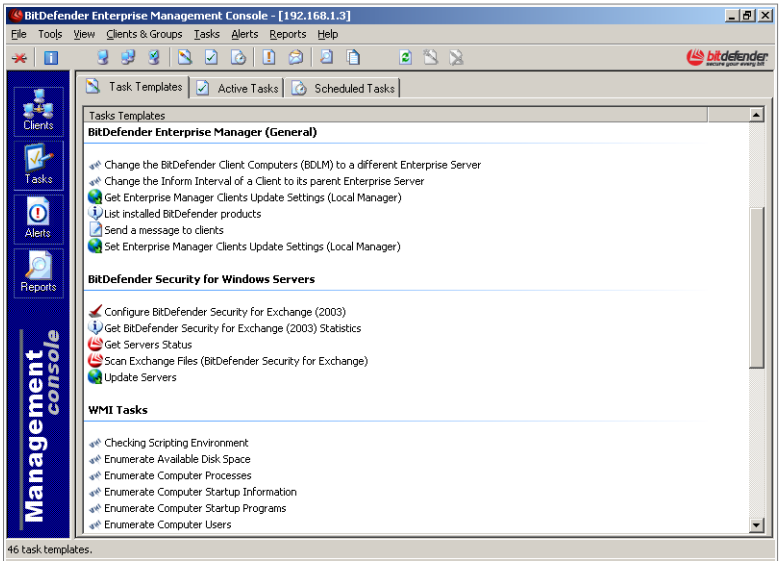
Follow the next steps to import the task templates for BitDefender Security for Exchange:

1. Access the **Clients** section. Do any of the following:
   - 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 **CTRL+1** shortcut.
2. Select a client on which **BitDefender Security for Exchange** is installed.
3. Import the task templates for BitDefender Security for Exchange using one of the following methods:
   - On the **Clients&Groups** menu, point to **Clients** and then click **Import Tasks Templates from Selected Clients**.
   - Right-click the selected client and then click **Import Tasks Templates from Selected Clients** on the shortcut menu.

The imported task templates will appear in the **Tasks Templates** section. To access it, do any of the following:

- Click **Tasks** from the configuration bar.
- On the **Tasks** menu, click **Go to Tasks Templates Pane**.

- Click the **Open Task Templates Pane** button from the toolbar.
- Use the **CTRL+4** shortcut.



Additional Task Templates

This is where you can see the available task templates for all BitDefender clients. Double-click a task template to launch the wizard that will help you configure a task.

The additional task templates for BitDefender Security for Exchange are listed under the **BitDefender Security for Windows Servers** heading. The following additional task templates are available:

- Configure BitDefender Security for Exchange - to configure the BitDefender Security for Exchange products installed on one or more servers.
- Get BitDefender Security for Exchange Statistics - to obtain statistics about the activity of the BitDefender Security for Exchange products installed on one or more servers.
- Get Servers Status - to obtain information about the status of the BitDefender products installed on one or more servers.

- Scan Exchange Files (BitDefender Security for Exchange) - to scan the files of the Exchange Servers on which BitDefender Security for Exchange is installed.
- Update Servers - to update the BitDefender products installed on one or more servers.

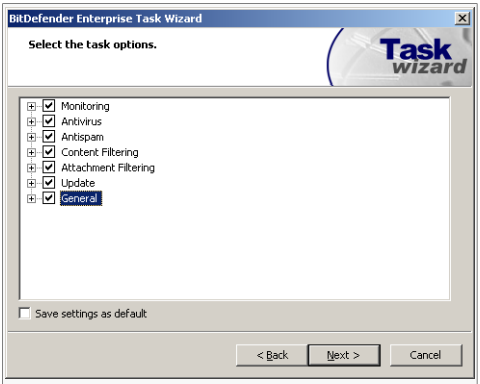
18.1. Configure BitDefender Security for Exchange

In order to configure the **BitDefender Security for Exchange** products installed on one or more clients, double-click **Configure BitDefender Security for Exchange** (in the **Task Templates** pane). This will launch the wizard which will guide you through the task configuration process:

18.1.1. Step 1/5 - Welcome to BitDefender Task Wizard

Click **Next** to continue or **Cancel** to quit the configuration.

18.1.2. Step 2/5 - Select Task Options



Select the task options

Here you can configure all BitDefender Security for Exchange options.

The configuration options are grouped into 7 main categories: Monitoring, Antivirus, Antispam, Content Filtering, Attachment Filtering, Update and General.

Note

Click the box labeled "+" to open a category or click the one labeled "-" to close it. You may notice that some options cannot be opened although the "+" sign appears next to them. This is due to the fact that these options have not been selected yet. You will notice that once selected, such options can be opened.

Monitoring

Check **Monitoring** in order to set up the configuration options for the mail and net send notification services, BitDefender log file and quarantine folder. These options appear in the **Monitoring** module.

The following options are available:

- **Alerts** - to configure the mail and net send notification services.
  - **Mail Alerts** - to configure the mail notification service.
    - **Enable** - enables the mail notification service.
    - **Mail server** - allows specifying the settings required to send mail alerts.

Click **SMTP Server** and provide the IP address of the SMTP server that your network uses to send messages. Click **From address** and specify the e-mail address that will appear in the sender field.

- **Global alert receivers** - click this link to specify the e-mail addresses of the global receivers of the mail alerts. The e-mail addresses must be separated by a semicolon (";"). They will appear between angle brackets.

- **Net Send Alerts** - to configure the net send notification service.
  - **Enable** - enables the net send notification service.
  - **List of computer names** - click this link to specify the computer names to which the net send alerts will always be sent. The names must be separated by a semicolon (";"). They will appear between angle brackets.

- **Log** - to configure the options for the BitDefender log file.
  - **Enable** - enables file logging.
  - **Change location** - to change the location where the log file is saved. Click this link and provide the path to the folder where the log files should be saved. The new location will appear between angle brackets.

- **Quarantine** - to set the locations of the quarantine folders.

  To specify the Antivirus, Antispam, Content Filtering or Attachment Filtering quarantine location, click the corresponding link and provide the path to the quarantine folder. The new location will appear between the angle brackets.

Antivirus

Check **Antivirus** in order to configure the **Antivirus** module.

The scanning options are grouped into two categories:

- Real time antivirus scan
- On-demand antivirus scan

Real-time Antivirus Scanning Settings

To configure the options for the real-time protection check **Real time antivirus scan**.

To enable real-time antivirus scanning check **Enable**.

You can specify the scanning option for the default rule:

- **Scan** - the messages to which the default rule applies will be scanned according to the antivirus scanning options specified by the rule.

- **Do not scan** - the messages to which the default rule applies will not be scanned using antivirus scanning options.

Note
The scanning option specified here will not apply to messages for which specific scanning policies have been created.

Check **First / Second action if virus found** to specify the action to be taken on infected messages. You must choose one of the following actions:

Action	Description
Disinfect	The infected message is disinfected. You can choose a second action to be taken on the infected messages if disinfection fails. The second action options are delete, quarantine, deliver mail (as defined below).
Delete mail	The infected message is deleted.
Replace	The infected object (mail body / attachment) is replaced with a specified text.
Quarantine and replace	The infected object (mail body / attachment) is moved to the quarantine folder and its content is replaced with a specified text.
Deliver	The infected message is delivered in full to its receivers.

Check **Notifications** to specify the notification options. To notify users about infected messages or messages that could not be scanned check the corresponding options.

Check **Advanced** to configure some advanced settings for the real-time protection. The following options are available:

- **Background scanning** - to enable background scanning.
- **Proactive scanning** - to enable proactive scanning.
- **Transport scanning** - to enable transport scanning.

Note
Available only on Microsoft Exchange Server 2003!

- **Scan rich text format** - to scan the body messages in RTF (Rich Text Format).

- **Scan plain text** - to scan body messages in plain text format.
- **Scan timeout** - to specify the maximum time allocated to scan an object.
- **Number of threads** - to specify the maximum number of threads to be used. The recommended number can be computed this way: `2*number of CPU+1`.
- **Maximum archive depth to scan** - to specify the maximum archive depth to scan. The recommended depth is 16.

On-demand Antivirus Scanning Settings

To configure the options for the on-demand scan check **On-demand antivirus scan**.

Check **Mailbox settings** to specify the items to be scanned. You can choose:

- **Scan all** - to scan all mailboxes and public folders of the Exchange server.
- **Custom scan** - to scan only the specified mailboxes and public folders. Double-click **List of mailboxes** / **List of public folders** and add a new item to be scanned.

Check **First / Second action if virus found** to specify the action to be taken on infected messages. You must choose one of the following actions:

Action	Description
Disinfect	The infected message is disinfected. You can choose a second action to be taken on the infected messages if disinfection fails. The second action options are delete, quarantine, deliver mail (as defined below).
Delete mail	The infected message is deleted.
Quarantine mail	The infected object (mail body / attachment) is moved to the quarantine folder and its content is replaced with a specified text.
Deliver mail	The infected message is delivered in full to its receivers.

Check **Notifications** to configure the notification options. The following options are available:

- **Log start/end of on-demand scan** - to record the start and the end of the scanning process in the log file.
- **Generate scan report** - to generate a report on the on-demand scan.

Click **Scan report location** and provide the path to the folder where the report file should be saved. The default location of the report file is: `C:\Program Files\Softwin\BitDefender Security for Exchange\Reports`.

You can choose the format of the report file from the menu. The report can be generated in HTML, text or CSV format.

If you only want the infected / suspect files to be logged in the report, check the corresponding option.

Antispam

Check **Antispam** in order to configure the **Antispam** module.

To enable the **Antispam** module, check **Enable**.

You can specify the filtering option of the default rule:

- **Scan** - the messages to which the default rule applies will be scanned according to the antispam filtering options specified by the rule.
- **Do not scan** - the messages to which the default rule applies will not be scanned using antispam filtering options.

Note

The filtering option specified here will not apply to messages for which specific filtering policies have been created.

Several antispam filtering settings can be configured for the default rule. Check an option in order to configure the settings corresponding to the respective category:

- **Antispam engines** - to specify which antispam engines to use to filter the messages to which the default rule applies.

  To enable the multi filter, check **Enable multi filter** and then the components you want to be enabled.

  To enable the Image filter, the URL filter, the NeuNet (Heuristic) filter or the Pre-trained Bayesian filter, check **Advanced filters** and then the filter you want to be enabled.
- **Actions** - to specify the action options for the default rule.

  You can specify the threshold level by selecting **Threshold** and then providing the desired value in the edit field. If you do not want to set a threshold, just select **Let BitDefender decide spam status** and BitDefender will decide by itself which messages are spam.

  The following actions are available on the **Action** list:

Action	Description
Deliver mail	Spam messages are delivered in full to their receivers.
Delete mail	Spam messages are deleted.
Quarantine	Spam messages are moved to the quarantine folder.
Redirect	Spam messages are redirected to a specified e-mail address. You must specify the e-mail address where the spam messages will be delivered in the **Mail address to redirect** field. If you want to provide more than one address, separate them by a semi-colon ";". If the field is empty or the e-mail address is invalid the messages will not be redirected.
Reject	Spam messages are rejected with a 550 SMTP error code.

In order to help you process spam messages, several additional actions are available:

Action	Description
Modify subject of spam	The subject of the messages detected as spam is modified. You can modify the subject pattern. We recommend you to use one of these patterns: • `[SPAM]${subject}[SPAM]` - to add `[SPAM]` before and after the subject. This is the default subject pattern. • `[SPAM]` - to replace the subject with `[SPAM]`. • `[$score% SPAM]$subject` - to add `[x SPAM]` before the subject, where `x` represents the spam score.
Add mail header	An e-mail header is added to the messages detected as spam. Provide the header name and the spam and non-spam values in the corresponding fields. By default, the spam and non-spam values are `${status} (${score})`. This means that for a spam

Action	Description
	message the header will be `Name: Yes(x)`, while for a legitimate message the header will be `Name: No(x)`, where `x` represents the spam score received by the message.
Save to folder	Spam messages are saved to a specified folder. Provide the folder location in the **Path** field.
Archive to account	Spam messages are archived to a specified account. Provide the e-mail archive address in the edit field. A Bcc containing the address will be added to the detected messages.

- **Enable White/Black lists** - to enable/disable the White List and the Black List configured for the default rule.
- **Bayesian filter** - to configure the Bayesian filter for the default rule.

  Check **Enable** if you want the messages to which the default rule applies to be analyzed by the Bayesian filter.

  Click **Ham folder** / **Spam folder** to specify the folders that contain the legitimate and the spam messages, respectively, on which the filter will be trained. To set the training time interval, click **Training interval** and indicate how frequently the filter should be trained, in minutes.
- **Advanced settings** - to specify which global filters to use to filter the messages to which the default rule applies.

  Check the global filters you want to use to filter the messages to which the default rule applies.

  If BitDefender protects a Microsoft Exchange Server 2003 client, you can choose to check authenticated connections by selecting the corresponding option.
- **First action when a virus is found** - select from the list the first action to be taken on infected objects:

First action	Description
Ignore	Ignore infected objects. No action taken.
Disinfect	Disinfect infected objects.
Delete	Delete infected objects.

First action	Description
Move to Quarantine	Isolate infected objects in the quarantine zone.

- **Second action to take when first fails** - select from the list the second action to be taken on infected files:

First action	Description
Ignore	Ignore infected objects. No action taken.
Delete	Delete infected objects.
Move to Quarantine	Isolate infected objects in the quarantine zone.

Note
This option is enabled only if the first action selected is **Disinfect**.

- **Quarantine folder** - type in the path to the quarantine area. This is required if the isolation of the infected objects in the quarantine area was selected.

Content Filtering

Check **Content Filtering** in order to configure the options of the **Content Filtering** module.

To enable the **Content Filtering** module, check **Enable**.

You can specify the filtering option of the default rule:

- **Scan** - the messages to which the default rule applies will be scanned according to the content filtering options specified by the rule.
- **Do not scan** - the messages to which the default rule applies will not be scanned using content filtering options.

Note
The filtering option specified here will not apply to messages for which specific filtering policies have been created.

Attachment Filtering

Check **Attachment Filtering** in order to configure the options of the **Attachment Filtering** module.

To enable the **Attachment Filtering** module, check **Enable**.

You can specify the filtering option of the default rule:

- **Scan** - the messages to which the default rule applies will be scanned according to the attachment filtering options specified by the rule.
- **Do not scan** - the messages to which the default rule applies will not be scanned using attachment filtering options.

Note

The filtering option specified here will not apply to messages for which specific filtering policies have been created.

Update

Check **Update** in order to configure the update options.

The update options are grouped into two categories:

- Settings
- Product Update

Settings

Check **Settings** to configure the automatic update options.

The following options are available:

- **Schedule** - check this option to specify when to perform updates. You can configure the following options:
  - **Enable automatic update** - enables the automatic update. This means BitDefender will be updated automatically, on a regular basis.
  - **Automatic update interval** - click this link and specify the number of hours between two consecutive checks for updates. The automatic update interval will appear between angle brackets.
  - **Enable Update Pushing** - enables Update Pushing. If this option is enabled, the update process will be triggered by special "Update Announcement Messages" sent by BitDefender.
- **Settings** - check this option to configure the update locations. You can configure the following options:
  - **Allow insecure updates** - allows updating BitDefender from local mirrors.
  - **First update location** - allows configuring a primary update location. If you are connected to a local network that has BitDefender virus and spyware signatures placed locally, you can change the location of the updates here.

To specify the update location, click **Update location** and provide the address of the update server. The official BitDefender update location is: `upgrade.bitdefender.com`.

In case the company uses a proxy server to connect to Internet, check **Use proxy**. The following settings must be specified:

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

- **Second update location** - allows configuring an alternative update location. It is possible to configure the same settings as for the first update location.

- **Notifications** - check this option to specify which update events to be alerted about, based on the product notification settings. You can check **Update information** to alert receivers about a successful update or if no update is available or **Update error** to alert receivers if an error occurred during the update process.

Product Update

Check **Product Update** and then **Notify when product update available** if you want to alert certain receivers when product updates are available, based on the product notification settings.

General

Check **General** in order to set up general options.

The following options are available:

- **Register** - to register the product. You must provide the license key in the **Registration key** field.
- **Dump Management** - to configure dump management settings.

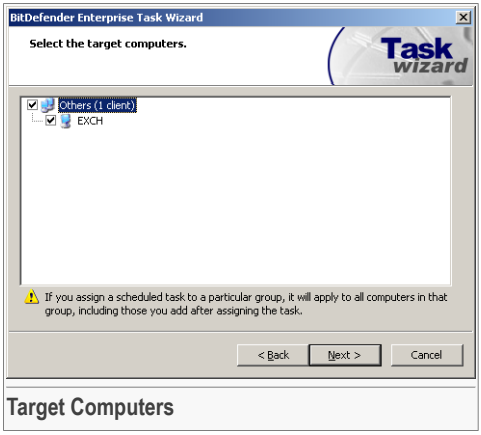
  To submit for analysis dumps created during BitDefender crashes, check **I agree to submit dumps to the BitDefender Lab** and provide your address in the **Mail address of dump sender**.
- **Virus Report** - to configure real-time virus reporting.

  To send reports about viruses and spyware found on the local computers, check **Enable** and select from the list the country you live in.

Check **Save settings as default** if you want to keep the same configuration for future tasks.

Click **Next**.

18.1.3. Step 3/5 - Select Target Computers



Target Computers

All clients and client groups are displayed here.

Note

Double-click a group to see the clients it contains.

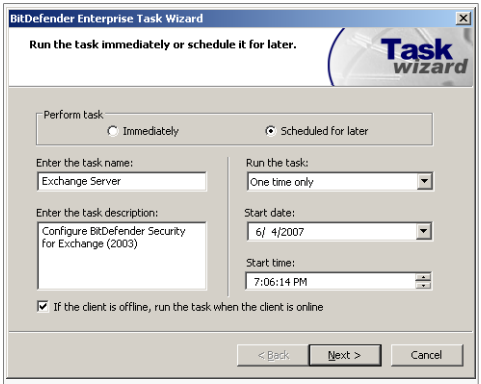
You can choose to run the task on one or several clients or client groups. Check the clients and/or the client groups on which this task will run.

Note

If you schedule a task to run on an entire client group, the task will run on all the clients of that group, including those added at a later time.

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

18.1.4. Step 4/5 - Set Task Schedule



Task Schedule

First, provide the task name and, optionally, the task description in the corresponding fields.

Then, choose the task type. You can opt for an immediate or a scheduled task.

For an immediate task, select **Immediately**.

For a scheduled task, select **Scheduled for later** and set the task schedule. The following fields must be configured:

- **Run the task** - specify when the task should run. The following options are available on the list:
  - **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 every 6 hours.
  - **Every 12 hours** - to run the task every 12 hours.
  - **Every day** - to run the task daily.
  - **Every two days (48 hours)** - to run the task every 2 days.
  - **Every three days (72 hours)** - to run the task every 3 days.
  - **Weekly** - to run the task weekly.
  - **Monthly** - to run the task monthly.
- **Start date** - provide the start date in the edit field or click the arrow to select it from a calendar.

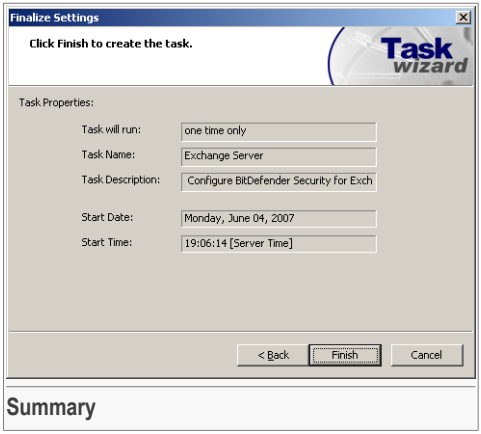
Note
The date format is month/day/year.

- **Start time** - provide the task launch time in the edit field or use the corresponding arrows to modify it.

Important
The task may fail if the target workstation is offline. To prevent this, check **If a client is offline, run the task when the client is online**.

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

18.1.5. Step 5/5 - Review Settings



Summary

The last window of the wizard contains all the information regarding the task. You can make any changes by returning to the previous steps (**Back**). If you do not want to make any changes, click **Finish**.

Depending on the run time you have selected, the task will appear either in the **Active Tasks** section, if it is an immediate task or in the **Scheduled Tasks** section, if it is a scheduled task.

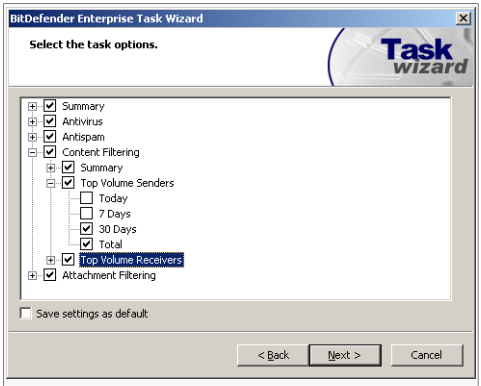
18.2. Get BitDefender Security for Exchange Statistics

In order to obtain statistics about the activity of the **BitDefender Security for Exchange** products installed on one or more clients, double-click **Get BitDefender Security for Exchange Statistics** (in the **Task Templates** pane). This will launch the wizard which will guide you through the task configuration process:

18.2.1. Step 1/5 - Welcome to BitDefender Task Wizard

Click **Next** to continue or **Cancel** to quit the configuration.

18.2.2. Step 2/5 - Select Task Options



Task Options

To get statistics on the product activity follow the next steps:

1. Choose what kind of statistics you want to obtain (**Summary**, **Antivirus**, **Antispam**, **Content Filtering** and / or **Attachment Filtering**).
2. Choose what type of statistics to obtain for each selected category.

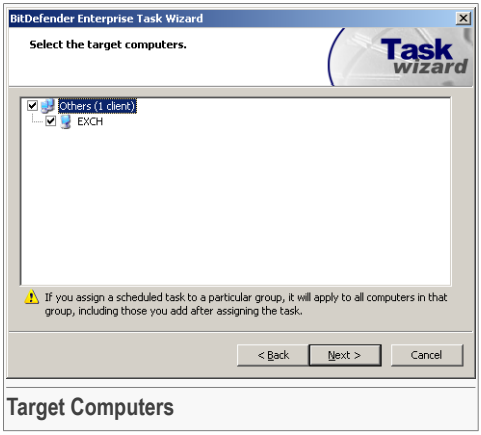
   For example, if you have selected only the **Content Filtering** category, you can choose **Summary**, **Top Volume Senders** and / or **Top Volume Receivers**.
3. Choose the time interval on which the statistics are generated (**Today**, **7 Days**, **30 Days** and / or **Total**).

Click **Next**.

Note

In order to see the results of this task, you must create a report from the **BitDefender Enterprise Manager** console. The statistics will be presented in a graphic mode.

18.2.3. Step 3/5 - Select Target Computers



Target Computers

All clients and client groups are displayed here.

Note

Double-click a group to see the clients it contains.

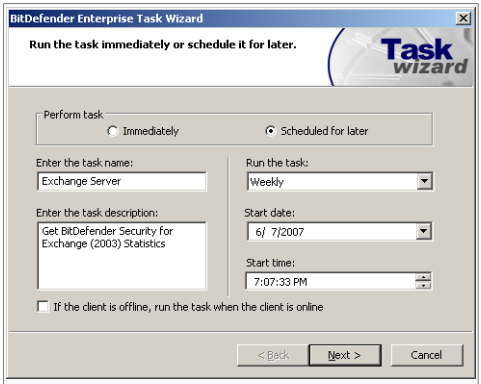
You can choose to run the task on one or several clients or client groups. Check the clients and/or the client groups on which this task will run.

Note

If you schedule a task to run on an entire client group, the task will run on all the clients of that group, including those added at a later time.

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

18.2.4. Step 4/5 - Set Task Schedule



Task Schedule

First, provide the task name and, optionally, the task description in the corresponding fields.

Then, choose the task type. You can opt for an immediate or a scheduled task.

For an immediate task, select **Immediately**.

For a scheduled task, select **Scheduled for later** and set the task schedule. The following fields must be configured:

- **Run the task** - specify when the task should run. The following options are available on the list:
  - **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 every 6 hours.
  - **Every 12 hours** - to run the task every 12 hours.
  - **Every day** - to run the task daily.
  - **Every two days (48 hours)** - to run the task every 2 days.
  - **Every three days (72 hours)** - to run the task every 3 days.
  - **Weekly** - to run the task weekly.
  - **Monthly** - to run the task monthly.
- **Start date** - provide the start date in the edit field or click the arrow to select it from a calendar.

Note

The date format is month/day/year.

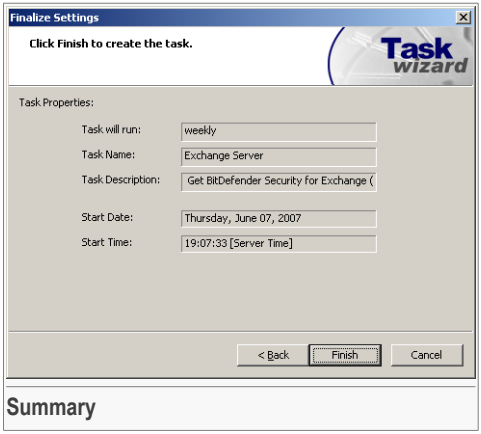
- **Start time** - provide the task launch time in the edit field or use the corresponding arrows to modify it.

Important

The task may fail if the target workstation is offline. To prevent this, check **If a client is offline, run the task when the client is online**.

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

18.2.5. Step 5/5 - Review Settings



Summary

The last window of the wizard contains all the information regarding the task. You can make any changes by returning to the previous steps (**Back**). If you do not want to make any changes, click **Finish**.

Depending on the run time you have selected, the task will appear either in the **Active Tasks** section, if it is an immediate task or in the **Scheduled Tasks** section, if it is a scheduled task.

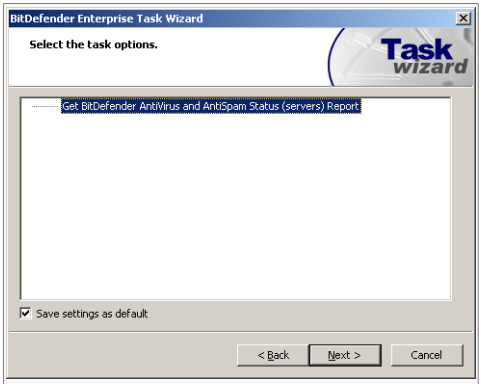
18.3. Get Servers Status

In order to obtain the status of the BitDefender server products installed on one or more clients, double-click **Get Servers Status** (in the **Task Templates** pane). This will launch the wizard which will guide you through the task configuration process:

18.3.1. Step 1/5 - Welcome to BitDefender Task Wizard

Click **Next** to continue or **Cancel** to quit the configuration.

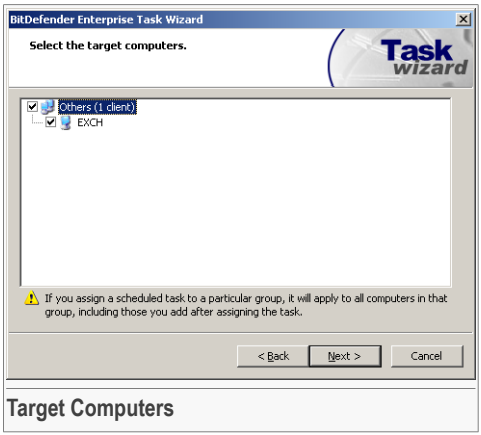
18.3.2. Step 2/5 - Select Task Options



Task Options

Click **Next**.

18.3.3. Step 3/5 - Select Target Computers



Target Computers

All clients and client groups are displayed here.

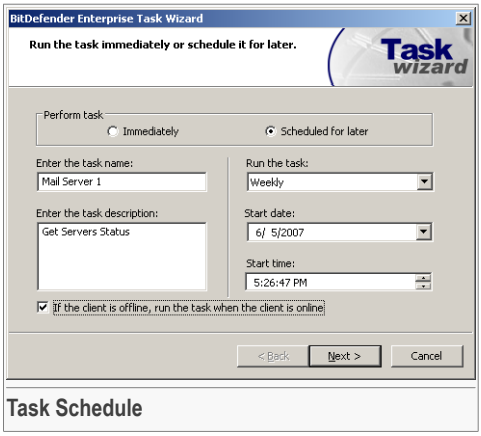
Note
Double-click a group to see the clients it contains.

You can choose to run the task on one or several clients or client groups. Check the clients and/or the client groups on which this task will run.

Note
If you schedule a task to run on an entire client group, the task will run on all the clients of that group, including those added at a later time.

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

18.3.4. Step 4/5 - Set Task Schedule



Task Schedule

First, provide the task name and, optionally, the task description in the corresponding fields.

Then, choose the task type. You can opt for an immediate or a scheduled task.

For an immediate task, select **Immediately**.

For a scheduled task, select **Scheduled for later** and set the task schedule. The following fields must be configured:

- **Run the task** - specify when the task should run. The following options are available on the list:
  - **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 every 6 hours.
- **Every 12 hours** - to run the task every 12 hours.
- **Every day** - to run the task daily.
- **Every two days (48 hours)** - to run the task every 2 days.
- **Every three days (72 hours)** - to run the task every 3 days.
- **Weekly** - to run the task weekly.
- **Monthly** - to run the task monthly.

- **Start date** - provide the start date in the edit field or click the arrow to select it from a calendar.

Note

The date format is month/day/year.

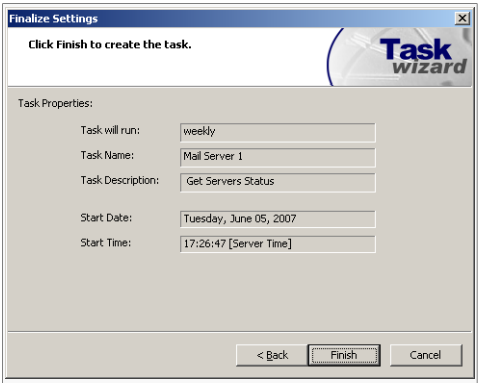
- **Start time** - provide the task launch time in the edit field or use the corresponding arrows to modify it.

Important

The task may fail if the target workstation is offline. To prevent this, check **If a client is offline, run the task when the client is online**.

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

18.3.5. Step 5/5 - Review Settings



Summary

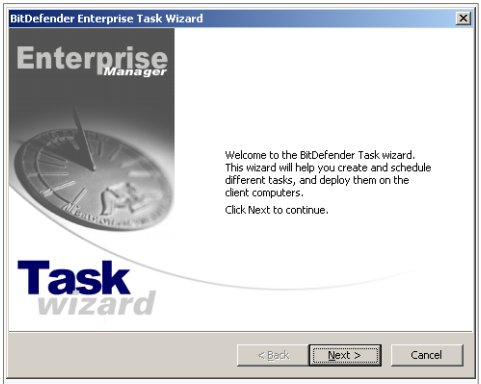
The last window of the wizard contains all the information regarding the task. You can make any changes by returning to the previous steps (**Back**). If you do not want to make any changes, click **Finish**.

Depending on the run time you have selected, the task will appear either in the **Active Tasks** section, if it is an immediate task or in the **Scheduled Tasks** section, if it is a scheduled task.

18.4. Scan Exchange Files (BitDefender Security for Exchange)

In order to scan the Exchange files of one or more Exchange servers clients having BitDefender Security for Exchange installed, double-click **Scan Exchange Files (BitDefender Security for Exchange)** (in the **Task Templates** pane). This will launch the wizard which will guide you through the task configuration process:

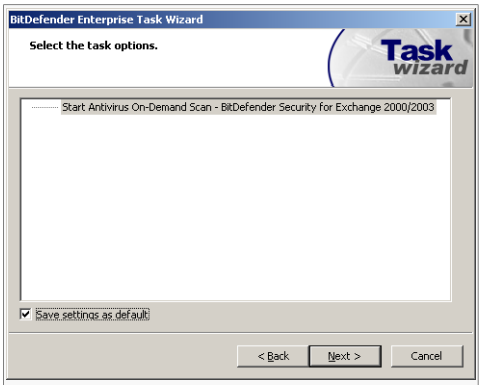
18.4.1. Step 1/5 - Welcome to BitDefender Task Wizard



Welcome

Click **Next** to continue or **Cancel** to quit the configuration.

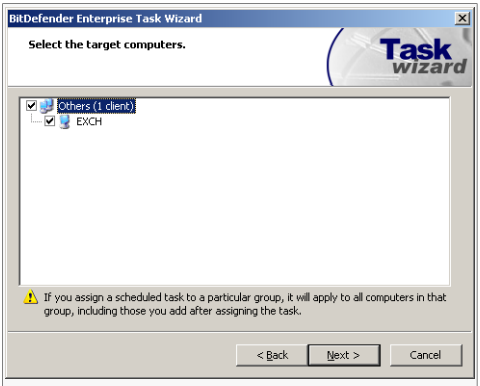
18.4.2. Step 2/5 - Select Task Options



Task Options

Click **Next**.

18.4.3. Step 3/5 - Select Target Computers



Target Computers

All clients and client groups are displayed here.

Note

Double-click a group to see the clients it contains.

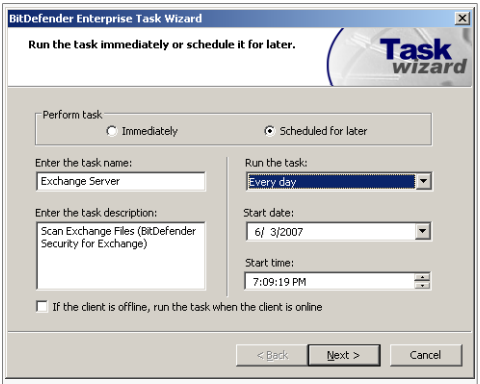
You can choose to run the task on one or several clients or client groups. Check the clients and/or the client groups on which this task will run.

Note

If you schedule a task to run on an entire client group, the task will run on all the clients of that group, including those added at a later time.

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

18.4.4. Step 4/5 - Set Task Schedule



Task Schedule

First, provide the task name and, optionally, the task description in the corresponding fields.

Then, choose the task type. You can opt for an immediate or a scheduled task.

For an immediate task, select **Immediately**.

For a scheduled task, select **Scheduled for later** and set the task schedule. The following fields must be configured:

- **Run the task** - specify when the task should run. The following options are available on the list:
  - **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 every 6 hours.
  - **Every 12 hours** - to run the task every 12 hours.
  - **Every day** - to run the task daily.
  - **Every two days (48 hours)** - to run the task every 2 days.
  - **Every three days (72 hours)** - to run the task every 3 days.
  - **Weekly** - to run the task weekly.
  - **Monthly** - to run the task monthly.
- **Start date** - provide the start date in the edit field or click the arrow to select it from a calendar.

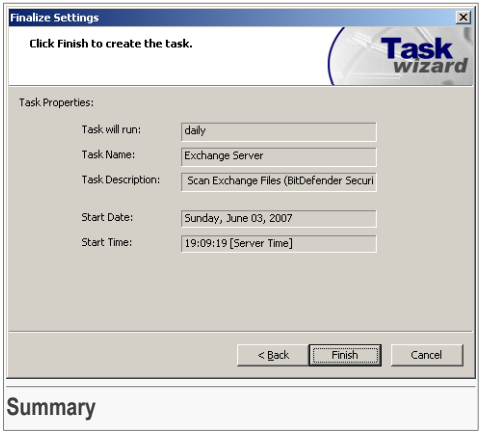
Note
The date format is month/day/year.

- **Start time** - provide the task launch time in the edit field or use the corresponding arrows to modify it.

Important
The task may fail if the target workstation is offline. To prevent this, check **If a client is offline, run the task when the client is online**.

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

18.4.5. Step 5/5 - Review Settings



Summary

The last window of the wizard contains all the information regarding the task. You can make any changes by returning to the previous steps (**Back**). If you do not want to make any changes, click **Finish**.

Depending on the run time you have selected, the task will appear either in the **Active Tasks** section, if it is an immediate task or in the **Scheduled Tasks** section, if it is a scheduled task.

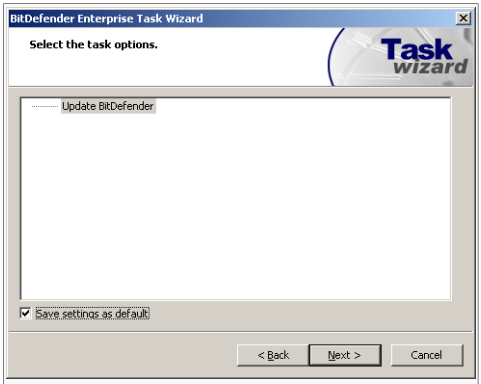
18.5. Update Servers

In order to update the BitDefender server products installed on one or more clients, double-click **Update Servers** (in the **Task Templates** pane). This will launch the wizard which will guide you through the task configuration process:

18.5.1. Step 1/5 - Welcome to BitDefender Task Wizard

Click **Next** to continue or **Cancel** to quit the configuration.

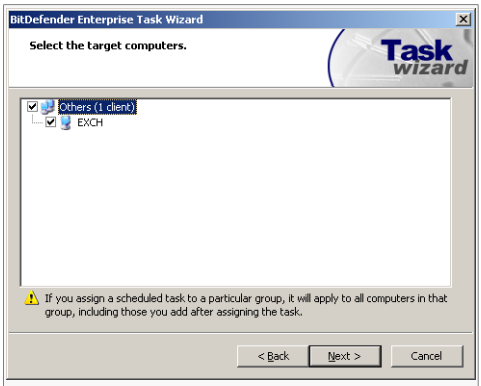
18.5.2. Step 2/5 - Select Task Options



Task Options

Click **Next**.

18.5.3. Step 3/5 - Select Target Computers



Target Computers

All clients and client groups are displayed here.

Note

Double-click a group to see the clients it contains.

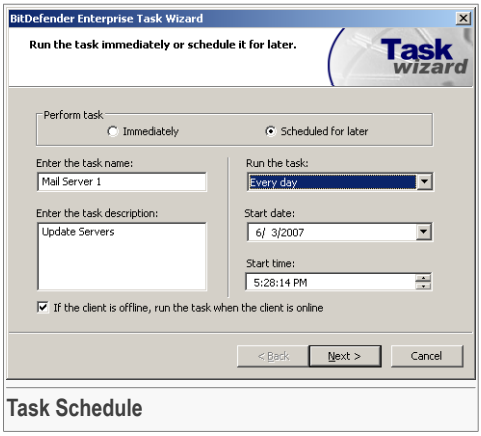
You can choose to run the task on one or several clients or client groups. Check the clients and/or the client groups on which this task will run.

Note

If you schedule a task to run on an entire client group, the task will run on all the clients of that group, including those added at a later time.

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

18.5.4. Step 4/5 - Set Task Schedule



Task Schedule

First, provide the task name and, optionally, the task description in the corresponding fields.

Then, choose the task type. You can opt for an immediate or a scheduled task.

For an immediate task, select **Immediately**.

For a scheduled task, select **Scheduled for later** and set the task schedule. The following fields must be configured:

- **Run the task** - specify when the task should run. The following options are available on the list:
  - **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 every 6 hours.
- **Every 12 hours** - to run the task every 12 hours.
- **Every day** - to run the task daily.
- **Every two days (48 hours)** - to run the task every 2 days.
- **Every three days (72 hours)** - to run the task every 3 days.
- **Weekly** - to run the task weekly.
- **Monthly** - to run the task monthly.

- **Start date** - provide the start date in the edit field or click the arrow to select it from a calendar.

Note

The date format is month/day/year.

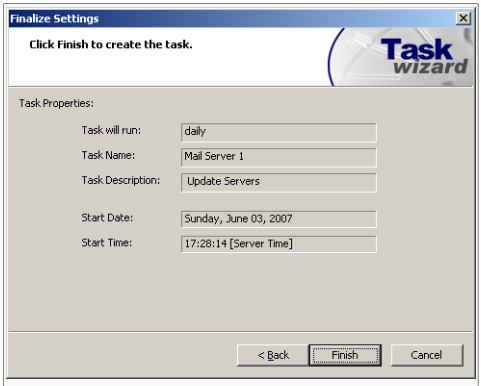
- **Start time** - provide the task launch time in the edit field or use the corresponding arrows to modify it.

Important

The task may fail if the target workstation is offline. To prevent this, check **If a client is offline, run the task when the client is online**.

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

18.5.5. Step 5/5 - Review Settings



Summary

The last window of the wizard contains all the information regarding the task. You can make any changes by returning to the previous steps (**Back**). If you do not want to make any changes, click **Finish**.

Depending on the run time you have selected, the task will appear either in the **Active Tasks** section, if it is an immediate task or in the **Scheduled Tasks** section, if it is a scheduled task.

Getting Help

19. Support

19.1. Support Department

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.

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

19.2. On-line Help

19.2.1. BitDefender Knowledge Base

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

The BitDefender Knowledge Base is open to the public and freely searchable. The extensive information it contains is yet another means of providing BitDefender customers with the technical knowledge and insight they need. All valid requests for information or bug reports coming from BitDefender clients eventually find their way into the BitDefender Knowledge Base, as bugfix reports, workaround cheatsheets or informational articles to supplement product helpfiles.

The BitDefender Knowledge Base is available any time at http://kb.bitdefender.com.

19.3. Contact Information

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.

19.3.1. Web Addresses

Sales department: <sales@bitdefender.com>
Technical support: <support@bitdefender.com>
Documentation: <documentation@bitdefender.com>
Partner Program: <partners@bitdefender.com>
Marketing: <marketing@bitdefender.com>
Media Relations: <pr@bitdefender.com>
Job Opportunities: <jobs@bitdefender.com>
Virus Submissions: <virus_submission@bitdefender.com>
Spam Submissions: <spam_submission@bitdefender.com>
Report Abuse: <abuse@bitdefender.com>
Product web site: http://www.bitdefender.com
Product ftp archives: ftp://ftp.bitdefender.com/pub
Local distributors: http://www.bitdefender.com/partner_list
BitDefender Knowledge Base: http://kb.bitdefender.com

19.3.2. Branch Offices

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

Germany

Softwin GmbH
Headquarter Western Europe
Karlsdorferstrasse 56
88069 Tettnang
Germany
Tel: +49 7542 9444 44
Fax: +49 7542 9444 99
Email: <info@bitdefender.com>
Sales: <sales@bitdefender.com>

Web: http://www.bitdefender.com
Technical Support: <support@bitdefender.com>

UK and Ireland

One Victoria Square
Birmingham
B1 1BD
Tel: +44 207 153 9959
Fax: +44 845 130 5069
Email: <info@bitdefender.com>
Sales: <sales@bitdefender.com>
Web: http://www.bitdefender.co.uk
Technical support: <support@bitdefender.com>

Spain

Constelación Negocial, S.L
C/ Balmes 195, 2a planta, 08006
Barcelona
Soporte técnico: <soporte@bitdefender-es.com>
Ventas: <comercial@bitdefender-es.com>
Phone: +34 932189615
Fax: +34 932179128
Sitio web del producto: http://www.bitdefender-es.com

U.S.A

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Technical support: <support@bitdefender.com>
Customer Service: 954-776-6262
Web: http://www.bitdefender.com

Romania

SOFTWIN
5th Fabrica de Glucoza St.
PO BOX 52-93
Bucharest
Technical support: <suport@bitdefender.ro>
Sales: <sales@bitdefender.ro>

Phone: +40 21 2330780
Fax: +40 21 2330763
Product web site: http://www.bitdefender.ro