bitdefender for MS ISA Servers Enterprise Edition

User's guide

Antivirus

Antispyware

bitdefender
secure your every bit

BitDefender for MS ISA Servers Enterprise Edition

User's guide

BitDefender

Published 2006.11.28
Version 2.0

Legal Notice

Warning and Disclaimer. This product and its documentation are protected by copyright. The information in this document is provided on an "as is" basis, without warranty. Although every precaution has been taken in the preparation of this document, the authors will not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

This book contains links to third-party Websites that are not under the control of SOFTWIN, and SOFTWIN is not responsible for the content of any linked site. If you access a third-party website mentioned in this guide, you will do so at your own risk. SOFTWIN provides these links only as a convenience, and the inclusion of the link does not imply that SOFTWIN endorses or accepts any responsibility for the content of those third-party sites.

Trademarks. Trademark names may appear in this book. All registered and unregistered trademarks in this document are the sole property of their respective owners.

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>.

Preface

This guide is intended to all companies who have chosen **BitDefender for MS ISA Servers Enterprise Edition** as a security solution for their MS ISA Servers Enterprise Edition computers. The information presented in this book is suitable not only for computer literates, it is accessible to everyone who is able to work under Windows.

This book will describe for you **BitDefender for MS ISA Servers Enterprise Edition**, the Company and the team who built it, will guide you through the installation process, will teach you how to configure it. You will find out how to use **BitDefender for MS ISA Servers Enterprise Edition**, how to update, test and customize it. You will learn how to get best from BitDefender.

We wish you a pleasant and useful lecture.

1. Conventions Used in This Book

1.1. Typographical Conventions

Several text styles are used in the book for an improved readability. Their aspect and meaning are presented in the table below.

Appearance	Description
`sample syntax`	Syntax samples are printed with `monospaced` characters.
http://www.bitdefender.com	The URL link is pointing to some external location, on http or ftp servers.
<support@bitdefender.com>	E-mail messages are inserted in the text for contact information.
"Preface" (p. xiii)	This is an internal link, towards some location inside the document.
`filename`	File and directories are printed using `monospaced` font.
option	All the product options are printed using **strong** characters.

1.2. Admonitions

The admonitions are in-text notes, graphically marked, bringing to your attention additional information related to the current paragraph.

Note

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

Important

This requires your attention and is not recommended to skip over it. Usually, it provides non-critical but significant information.

Warning

This is critical information you should treat with increased caution. Nothing bad will happen if you follow the indications. You should read and understand it, because it describes something extremely risky.

2. The Book Structure

The book consists of 7 parts, containing the major topics: About BitDefender, Product Installation, Description and Features, Management Console, Best Practices, BitDefender Enterprise Manager Integration and Getting Help.

About BitDefender. A short introduction to BitDefender. It explains who BitDefender and SOFTWIN are.

Product Installation. Step by step instructions for installing BitDefender on a workstation. This is a comprehensive tutorial on installing **BitDefender for MS ISA Servers Enterprise Edition**. Starting with the prerequisites for a successfully installation, you are guided through the whole installation process. Finally, the removing procedure is described in case you need to uninstall BitDefender.

Description and Features. The features and basic functionality of **BitDefender for MS ISA Servers Enterprise Edition** are presented to you. Also, a list of BitDefender products compatible with BitDefender for MS ISA Servers Enterprise Edition is provided.

Management Console. Description of basic administration and maintenance of BitDefender. The chapters explain in detail all options of **BitDefender for MS ISA Servers Enterprise Edition**, how to register the product, how to configure it, how to monitor its activity and how to perform the updates.

Best Practices. Follow the steps described in here in order to ensure antivirus and antispyware protection for web traffic.

BitDefender Enterprise Manager Integration. Description of BitDefender Enterprise Manager. Learn how to use BitDefender for MS ISA Servers Enterprise Edition through BitDefender Enterprise Manager.

Getting Help. Where to look and where to ask for help if something unexpected appears. It includes a FAQ section too.

3. Request for Comments

We invite you to help us improve the book. We have tested and verified all of the information to the best of our ability. Please write to tell us about any flaws you find in this book or how you think it could be improved, to help us provide you with the best documentation possible.

Let us know by sending an e-mail to <documentation@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.

1.2. About SOFTWIN

Founded in 1990, winner of the IST Prize in 2002, SOFTWIN is now considered to be the technological leader of the East-European software industry with annual growth rates of more than 50% in the past five years and 70% of annual turnover from exports.

With a team of over 800 qualified professionals, and more than 10000 projects managed so far, SOFTWIN focuses on providing complex software solutions and services which enable fast growing companies to solve critical business challenges and to take advantage of new business opportunities. The SOFTWIN development process is ISO 9001 certified.

As it is active on the most advanced IT markets of the US and European Union, SOFTWIN develops on 4 interlinked **business lines**:

- eContent Solutions
- BitDefender
- Business Information Solutions
- Customer Relationship Management

Product Installation

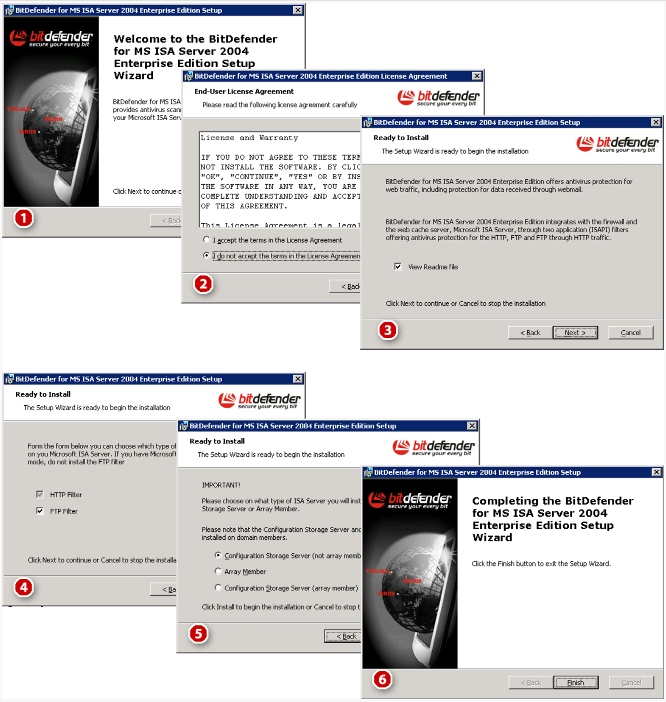
2. How to Install BitDefender for MS ISA Servers Enterprise Edition

2.1. System Requirements

Before installing the product, make sure that **Microsoft ISA Server 2004 Enterprise Edition** is installed on your server.

2.2. The Setup Wizard

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


BitDefender for MS ISA Server 2004 Enterprise Edition Setup
bitdefender secure your every bit
1
< Back
BitDefender for MS ISA Server 2004 Enterprise Edition License Agreement
2
< Back
3
< Back
Next >
Cancel
4
< Ba
5
< Back
6
< Back
Finish
Cancel
TROJAN
WORM
VIRUS

1 Welcome to the BitDefender for MS ISA Server 2004 Enterprise Edition Setup Wizard

BitDefender for MS ISA provides antivirus scann your Microsoft ISA Serv

Click Next to continue c

2 End-User License Agreement

Please read the following license agreement carefully

```
License and Warranty

IF YOU DO NOT AGREE TO THESE TERM
NOT INSTALL THE SOFTWARE. BY CLIC
"OK", "CONTINUE", "YES" OR BY INS
THE SOFTWARE IN ANY WAY, YOU ARE
COMPLETE UNDERSTANDING AND ACCEPT
OF THIS AGREEMENT.

This License Agreement is a legal
```

○ I accept the terms in the License Agreement

● I do not accept the terms in the License Agreemen

3 Ready to Install

The Setup Wizard is ready to begin the installation

BitDefender for MS ISA Server 2004 Enterprise Edition offers antivirus protection for web traffic, including protection for data received through webmail.

BitDefender for MS ISA Server 2004 Enterprise Edition integrates with the firewall and the web cache server, Microsoft ISA Server, through two application (ISAPI) filters offering antivirus protection for the HTTP, FTP and FTP through HTTP traffic.

☑ View Readme file

Click Next to continue or Cancel to stop the installation

4 Ready to Install

The Setup Wizard is ready to begin the installation

Form the form below you can choose which type of on you Microsoft ISA Server. If you have Microsoft mode, do not install the FTP filter

☑ HTTP Filter

☑ FTP Filter

Click Next to continue or Cancel to stop the installa

5 Ready to Install

The Setup Wizard is ready to begin the installation

IMPORTANT!

Please choose on what type of ISA Server you will inst Storage Server or Array Member.

Please note that the Configuration Storage Server anc installed on domain members.

● Configuration Storage Server (not array memb

○ Array Member

○ Configuration Storage Server (array member)

Click Install to begin the installation or Cancel to stop t

6 Completing the BitDefender for MS ISA Server 2004 Enterprise Edition Setup Wizard

Click the Finish button to exit the Setup Wizard.

The Setup Wizard

1. Click **Next** to continue or **Cancel** to quit the installation process.
2. Please read the License Agreement, select **I accept the terms in the License Agreement** and click **Next**. If you do not agree with these terms click **Cancel**. The installation process will be abandoned and you will exit the setup.
3. Check the box next to **View Readme file** if you want to see the readme file at the end of the installation process.

   Click **Next**.
4. Choose what type of BitDefender Antivirus filter to install: HTTP or FTP.
   - **HTTP Filter** - to install the HTTP filter.
   - **FTP Filter** - to install the FTP filter.

Warning

Do not install the FTP filter if you have MS ISA Servers Enterprise Edition installed in the Web Proxy mode!

Click **Next**.

5. Choose the type of ISA Server BitDefender is installed on:
   - **Configuration Storage Server (not array member)** - to register the filters on MS ISA Servers Enterprise Edition.
   - **Array Member** - to install BitDefender on an array member.
   - **Configuration Storage Server (array member)** - to register the filters and install BitDefender on a Configuration Storage Server which is a member of an array.

   Click **Install** in order to start installing the product.
6. Click **Finish** to complete the installation process.

Note

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

2.3. Installing the Product

For a quick and proper installation of the product, follow the installation steps below:

1. **Install BitDefender for MS ISA Servers Enterprise Edition on the Configuration Storage Server.**
   - If the Configuration Storage Server is installed on an array member, when reaching the fifth step of the wizard, select the **Configuration Storage Server (array member)** option.
   - If the Configuration Storage Server is installed on a computer which is not an array member, when reaching the fifth step of the wizard select the **Configuration Storage Server (not array member)** option.

Important

If you have a multiple array configuration, the filters will be registered on all arrays. If you do not want specific arrays to be protected with BitDefender specific arrays, please disable the BitDefender HTTP and FTP Filters from the Microsoft ISA 2004 Enterprise Server user interface.

2. **Install BitDefender for MS ISA Servers Enterprise Edition on the array members.**

- When reaching the fifth step of the wizard, select the **Array member** option.

  Important

  Select this option even if you have installed a Backup Configuration Storage Server on the array member. **BitDefender for MS ISA Servers Enterprise Edition** does not interfere in any way with the Backup Configuration Storage Server.

Note

You do not need to install **BitDefender for MS ISA Servers Enterprise Edition** on a stand-alone Backup Configuration Storage Server.

2.4. Uninstalling or Repairing BitDefender

Before uninstalling or repairing **BitDefender for MS ISA Servers Enterprise Edition**, go to the MS ISA Servers Enterprise Edition interface and access the **Firewall Policy** section. Double-click the rules which include FTP filtering to access their properties and click the **Protocols** tab. Choose **FTP** from the list and click **Edit**. In the window that will open, click the **Parameters** tab and uncheck the box next to **BitDefender Filter**.

Important

It is recommended that you uninstall **BitDefender for MS ISA Servers Enterprise Edition** first from the array members and only afterwards from the Configuration Storage Server.

If you want to repair or uninstall the previously installed **BitDefender for MS ISA Servers Enterprise Edition** open the Windows menu and follow the path **Start** -> **Programs** -> **BitDefender for MS ISA Servers** -> **Repair or Uninstall**.

A new window will appear where you can select:

- **Repair** - to re-install all program components installed during the previous setup.
- **Remove** - to remove all installed components.

Warning

When uninstalling **BitDefender for MS ISA Servers Enterprise Edition** from the array members, the Windows Firewall service will not restart automatically. Manual start is required.

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

Description and Features

3. Main Features

BitDefender for MS ISA Servers Enterprise Edition offers antivirus and antispyware protection for web traffic, including files received via web mail.

Improved Virus and Spyware Detection. Heuristic detection and proactive behavior blocking, coupled with lightning-fast updates of the signature lists make BitDefender for MS ISA Servers Enterprise Edition a reliable solution for corporate environments.

Certified Antivirus and Antispyware Engines. The award winning BitDefender scanning engines are acknowledged to provide the most proactive antivirus protection and feature the ground-breaking B-HAVE technology. BitDefender Antivirus and Antispyware scan engines are certified by ICSA Labs, Virus Bulletin, Checkmark, CheckVir and TÜV.

Behavioral Heuristic Analyzer in Virtual Environments. Behavioral Heuristic Analyzer in Virtual Environments (B-HAVE) emulates a virtual computer-inside-a-computer where pieces of software are run in order to check for potential malware behavior. This BitDefender proprietary technology represents a new security layer that keeps the operating system safe from unknown viruses by detecting malicious pieces of code for which signatures have not been released yet.

Antispyware Protection. BitDefender for MS ISA Servers Enterprise Edition makes use of a comprehensive database of spyware signatures to filter traffic and protect clients against such threats.

Integrated with MS ISA Servers Enterprise Edition. BitDefender for MS ISA Servers Enterprise Edition seamlessly integrates with MS ISA Servers Enterprise Edition through two application filters, an HTTP and an FTP filter.

Protection for Server Arrays. BitDefender for MS ISA Servers Enterprise Edition protects all the arrays of the enterprise that run MS ISA Servers Enterprise Edition.

HTTP and FTP Filters. The HTTP and FTP filters are application (ISAPI) filters that scan for viruses all HTTP and FTP requests. Depending on the rules set in the content filter and on the scan results, such requests are forwarded to the ISA Firewall Service.

Filter Management. BitDefender for MS ISA Servers Enterprise Edition offers administrators policy controls for virus protection and the ability to set specific filtering rules for specific groups of IP addresses across multiple scan types, thus improving the flexibility of the scanning and configuration process.

Browser Comforting. Due to the browser comforting feature, the end user does not perceive the very small overhead implied by the antivirus and antispyware scanning of all HTTP traffic, as chunks of the requested data are sent to the browser while the download is in progress.

White List Filter. A system of safe URL white lists, configurable by the administrator, is also available so that the traffic between the ISA Server and those specific URLs is not scanned.

Easy-to-use Interface. The new BitDefender for MS ISA Servers Enterprise Edition comes with an MMC based interface that offers a friendly working environment. The wizard system implemented in the interface enhances the usability of the product while the snap-in system provides the actual management functionality.

Interface Integration. BitDefender is integrated in the Microsoft ISA Server Console through two snap-ins that allow the configuration of the FTP and of the HTTP filter.

Remote Administration. BitDefender for MS ISA Servers Enterprise Edition enables the administration of the ISA Server computers from other computers. Remote administration can be performed either through a Terminal Services client, such as Remote Desktop Connection, or from a BitDefender MMC interface installed on a remote computer.

Automatic Updating. BitDefender for MS ISA Servers Enterprise Edition offers intelligent updates for virus definitions and the restricted content databases. Due to the advanced BitDefender technology implemented in the update module, the antivirus and antispyware protection is not discontinued during the update process.

Secures Infected or Suspected Files. Infected or suspected files are isolated in quarantine zones. The content of the quarantine zones can be analyzed at any time by the IT manager or can be sent for analysis to the BitDefender Labs.

Reports and Notifications. BitDefender for MS ISA Servers Enterprise Edition comes with useful “Reports” and “Statistics” modules that provide detailed information about the scanned files. The “Alerts” module is a tool used to alert the administrator in case of a virus, warning or error.

Centralized Management and Monitoring of the Server Arrays. BitDefender for MS ISA Servers Enterprise Edition is fully compatible with BitDefender Enterprise Manager, offering organizations centralized management for antivirus and antispyware protection and security policies inside complex networks. All the arrays and their members can be managed and monitored from a centralized location.

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

Professional Technical Support. Professional technical support is offered by qualified support representatives, supplemented by an online database with answers to Frequently Asked Questions and fixes for common issues.

4. How Does It Work?

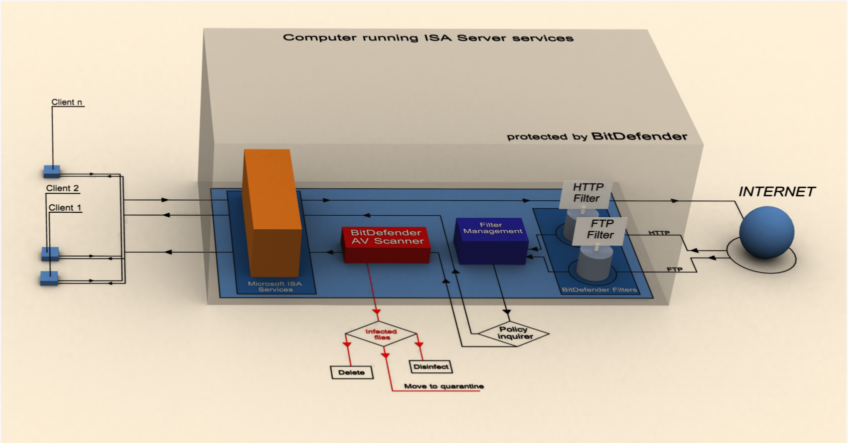
As content entering or leaving your company must meet security policies, it is crucial to choose the appropriate protection for each network level, especially for the gateway level. The World Wide Web has become an entry point for malicious content, through file transfers or simple browsing.

BitDefender for MS ISA Servers Enterprise Edition offers antivirus and antispyware protection for web traffic, including files received via web mail. **BitDefender for MS ISA Servers Enterprise Edition** integrates with the Microsoft Firewall Service through two application (ISAPI) filters offering antivirus and antispyware protection for HTTP, FTP and FTP through HTTP traffic.

BitDefender for MS ISA Servers Enterprise Edition is compatible with BitDefender for Mail Servers (WIN SMTP Proxy) which offers antivirus and antispam protection for SMTP traffic.

4.1. Working Schema

The design below shows how BitDefender works on a computer running ISA Server services:



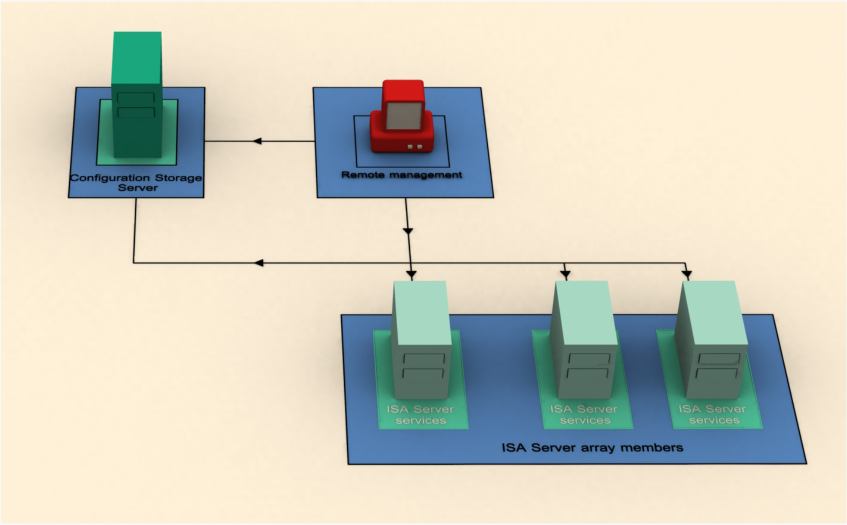
Working Schema

BitDefender intercepts downloaded files through the HTTP protocol, and downloaded or uploaded files through the FTP protocol, and such files are then scanned or not according to the rules defined by the manager/administrator in the Rules section.

Based on the administrator's option, infected files are disinfected, deleted or isolated on a certain location (the quarantine zone).

If a file is infected and it cannot be disinfected, it is blocked and an error message is sent to the user.

To understand how BitDefender works on MS ISA Servers Enterprise Edition, see the design below:



Working Schema

BitDefender for MS ISA Servers Enterprise Edition protects the entire array by registering the HTTP and FTP filters, for all array members, on the Configuration Storage Server. **BitDefender for MS ISA Servers Enterprise Edition** can be administered either remotely, from the management console of BitDefender Enterprise Manager, or directly, from the respective computer. The advantage of using **BitDefender Enterprise Manager** is that all BitDefender products can be configured and monitored from only one terminal, which saves time and money.

5. Compatibility with other BitDefender Products

BitDefender for MS ISA Servers Enterprise Edition offers antivirus and antispyware protection for the web traffic on the company servers, webmail data included. To ensure a complete protection of the servers at all levels, **BitDefender for MS ISA Servers Enterprise Edition** can be used simultaneously with other BitDefender server products.

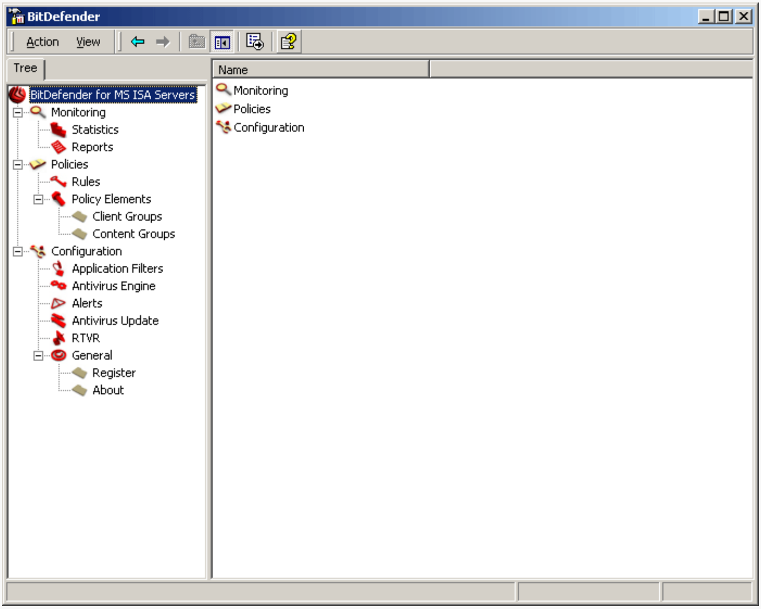
Here is a list of the BitDefender server products compatible with **BitDefender for MS ISA Servers Enterprise Edition**:

- **BitDefender v1.9, v2.0 for File Servers** - addresses the issues of data security and system availability on file servers;
- **BitDefender v1.9 for MS Exchange 2000** - provides antivirus & antispam protection deeply integrated with the MS Exchange 2000 server;
- **BitDefender v1.9 for MS Exchange 2003** - provides antivirus & antispam protection deeply integrated with the MS Exchange 2003 server;
- **BitDefender v1.9 for Mail Servers (Win SMTP Proxy)** - provides e-mail servers with a pro-active protection of the message traffic against viruses, Trojans or other potentially malicious code;
- **BitDefender v2.0 for SharePoint 2003** - provides antivirus protection of the SharePoint Server.

Management Console

6. Overview

The management console is accessed through the Windows Start menu, by following the path **Start** -> **Programs** -> **BitDefender for MS ISA Servers** -> **BitDefender for MS ISA Servers**.



Management Console

BitDefender for MS ISA Servers Enterprise Edition comes with an MMC based interface on the left-hand side of which the following sections are listed:

- Monitoring - Access to the **Monitoring** module.
  - Statistics - Access to the section containing statistics on the antivirus activity.
  - Reports - Access to the section where you can create and see the report files.
- Policies - Access to the **Policy** module.
  - Rules - Access to the section where you can define specific filtering rules.
  - Policy Elements - Access to the **Policy Elements** section.
    - Client Groups - Access to the section where you can create custom client groups.

    - Content Groups - Access to the section where you can create content type groups.

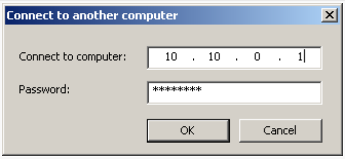
- Configuration - Access to the **Configuration** module.
  - Application Filters - Access to the section where you can configure the HTTP and FTP filters.
  - Antivirus Engine - Access to the section where you can select the actions to be taken on infected files.
  - Alerts - Access to the section where you configure alerts.
  - Antivirus Update - Access to the section where you configure product updates.
  - RTVR - Access to the section where you configure the real time virus reporting feature.
  - General - Access to the **General** section.
    - Register - Access to the section where you can register the product.
    - About - Access to the section where you can see product details.

If you want to open the help file, go to the Windows Start menu and follow this path: **Start -> Programs -> BitDefender for MS ISA Servers -> BitDefender Help**.

6.1. Contextual Menu

The contextual menu contains 2 important options:

- **Connect to another computer** - opens a window where you can specify the server IP and password.



Connect to another computer

Connect to computer: 10 . 10 . 0 . 1

Password: ********

Connect to another computer

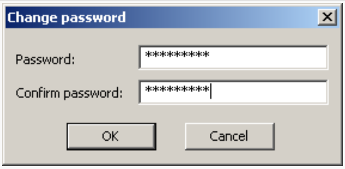
Type the server IP in the **Connect to computer** field and the password in the **Password** field.

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 password.



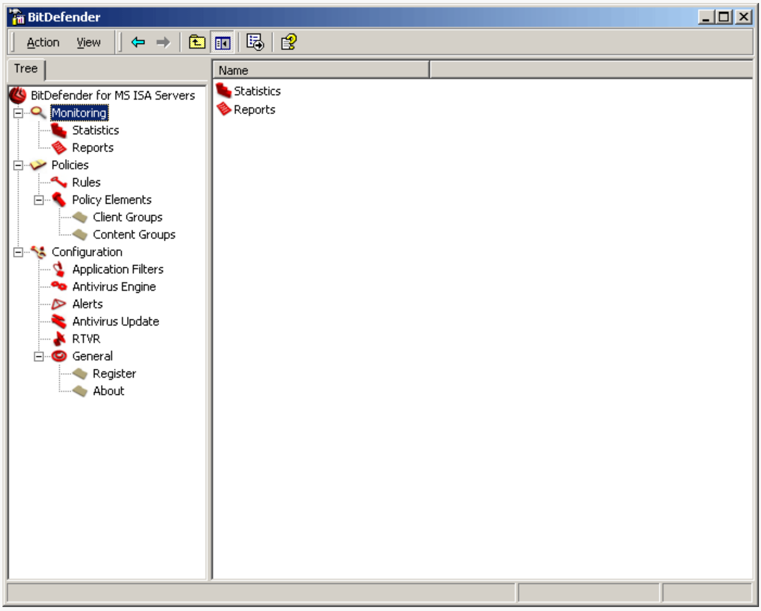
Change administrative password

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

Click **OK**.

7. Monitoring Module

Click the **Monitoring** tab on the management console. The following window will appear:



Monitoring Module

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

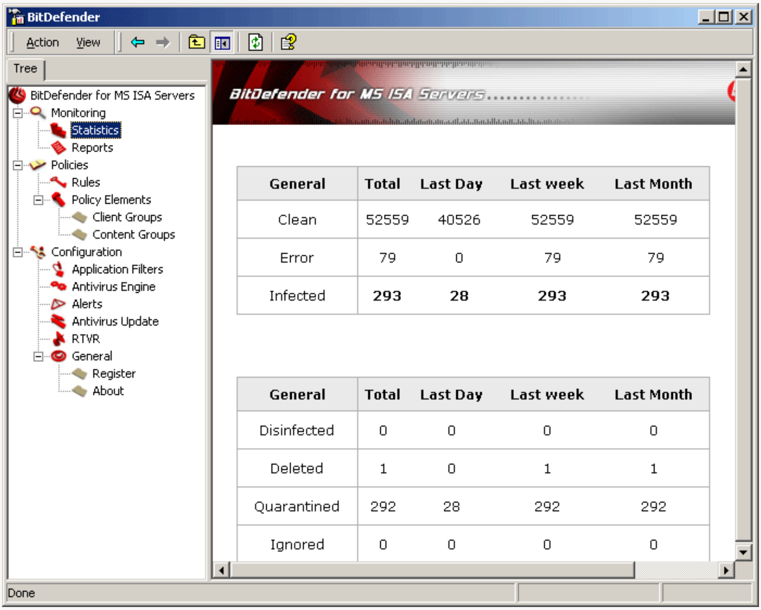
- Statistics
- Reports

Note

Right-click the **Monitoring** tab on the management console and select the **Clear all records** option from the contextual menu in order to delete all the records generated by this module.

7.1. Statistics

Click the **Statistics** tab on the management console (**Monitoring** module). The following window will appear:



General	Total	Last Day	Last week	Last Month
Clean	52559	40526	52559	52559
Error	79	0	79	79
Infected	**293**	**28**	**293**	**293**

General	Total	Last Day	Last week	Last Month
Disinfected	0	0	0	0
Deleted	1	0	1	1
Quarantined	292	28	292	292
Ignored	0	0	0	0

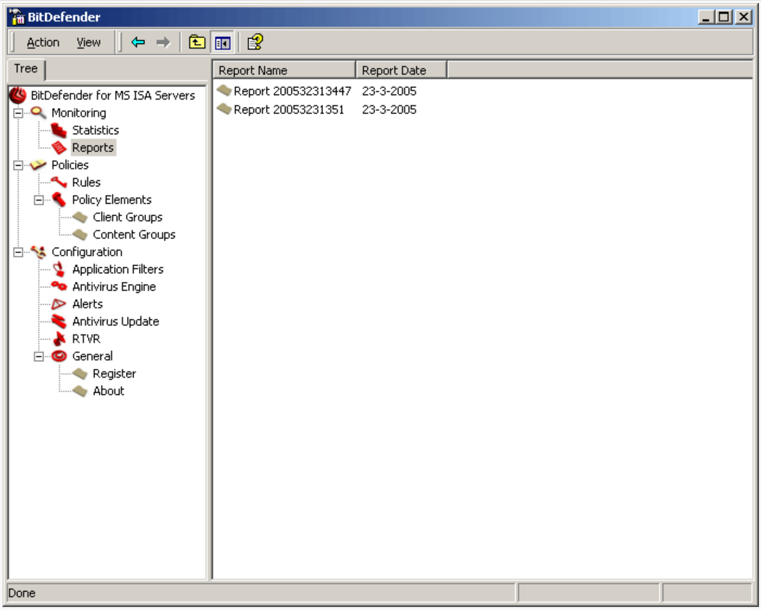
Statistics

The first table shown in this window presents statistic data on the antivirus activity conducted on your Microsoft ISA Server.

The second table presents the actions BitDefender took on infected objects.

7.2. Reports

Click the **Reports** tab on the management console (**Monitoring** module). The following window will appear:



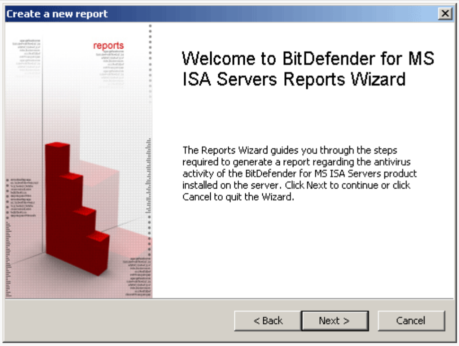
Report Name	Report Date
Report 200532313447	23-3-2005
Report 20053231351	23-3-2005

Reports

7.2.1. Reports Wizard

To create report files on the antivirus activity conducted over a certain period of time, you must run the **Reports Wizard** (on the contextual menu, point **New** and select **Create a new report**). The wizard is a five step procedure.

Step 1/5 - Welcome to the reports wizard



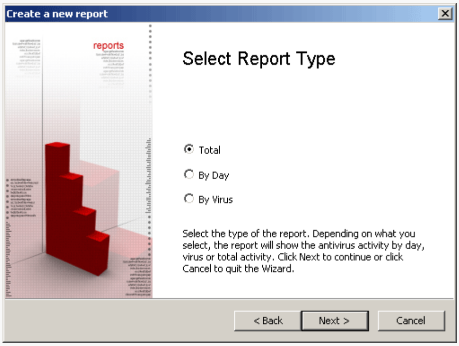
Welcome to BitDefender for MS ISA Servers Reports Wizard

The Reports Wizard guides you through the steps required to generate a report regarding the antivirus activity of the BitDefender for MS ISA Servers product installed on the server. Click Next to continue or click Cancel to quit the Wizard.

Welcome to the reports wizard

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

Step 2/5 - Select the report type



Select Report Type

● Total

○ By Day

○ By Virus

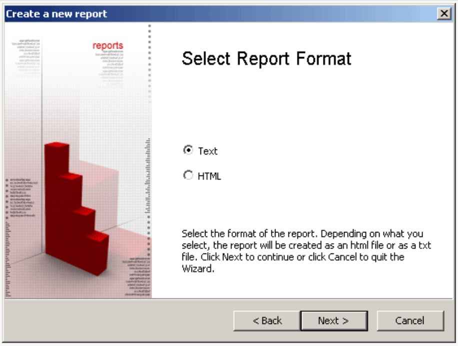
Select the type of the report. Depending on what you select, the report will show the antivirus activity by day, virus or total activity. Click Next to continue or click Cancel to quit the Wizard.

Select the report type

Select the report type: **Total**, **By Day**, or **By Virus**.

Click **Next**.

Step 3/5 - Select the report format



Select Report Format

● Text

○ HTML

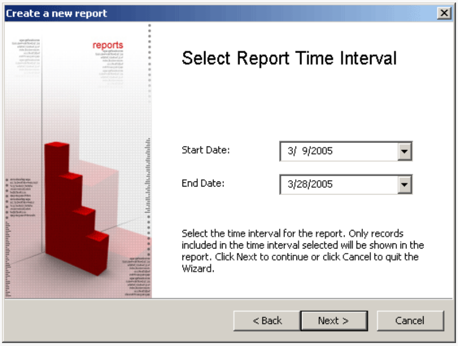
Select the format of the report. Depending on what you select, the report will be created as an html file or as a txt file. Click Next to continue or click Cancel to quit the Wizard.

Select the report format

Select the report format (text or HTML).

Click **Next**.

Step 4/5 - Select the time interval for the report



Select Report Time Interval

Start Date: 3/ 9/2005

End Date: 3/28/2005

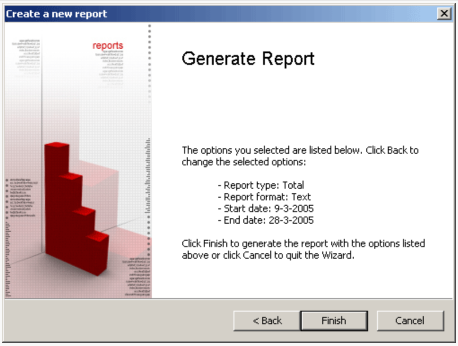
Select the time interval for the report. Only records included in the time interval selected will be shown in the report. Click Next to continue or click Cancel to quit the Wizard.

Select the time interval for the report

Select the time interval (**Start Date** and **End Date**) for the report.

Click **Next**.

Step 5/5 - See the summary



Generate Report

The options you selected are listed below. Click Back to change the selected options:

- Report type: Total
- Report format: Text
- Start date: 9-3-2005
- End date: 28-3-2005

Click Finish to generate the report with the options listed above or click Cancel to quit the Wizard.

See the summary

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

The report will appear in the Reports section.

Note

Only the last 12 reports will appear in this section.

7.2.2. Contextual Menu

Right-click a report to access a contextual menu containing the following options:

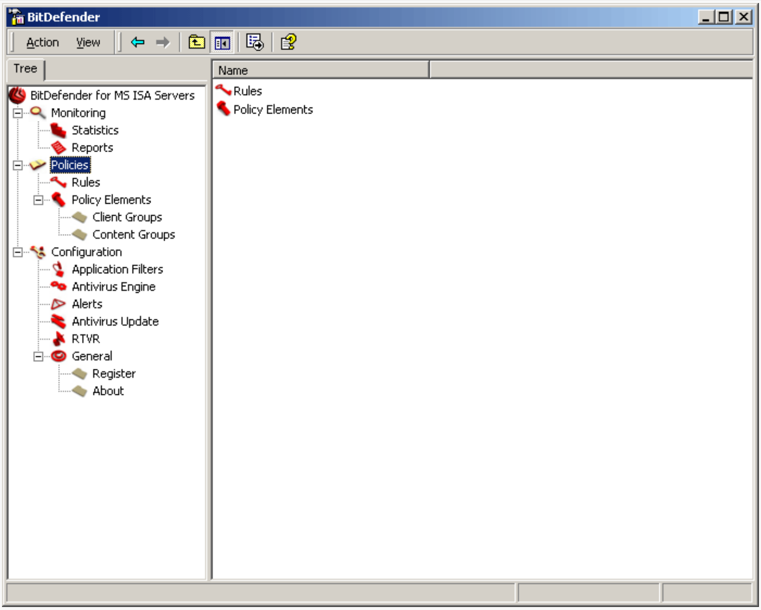
- **View Report** - open selected report file;
- **Save Report** - save selected report file;
- **Delete** - delete selected report file;
- **Help** - open help file.

Note

Right-click the **Reports** tab on the management console and select the **Delete all reports** option from the contextual menu in order to delete all the reports generated so far.

8. Policies Module

Click the **Policies** tab on the management console. The following window will appear:



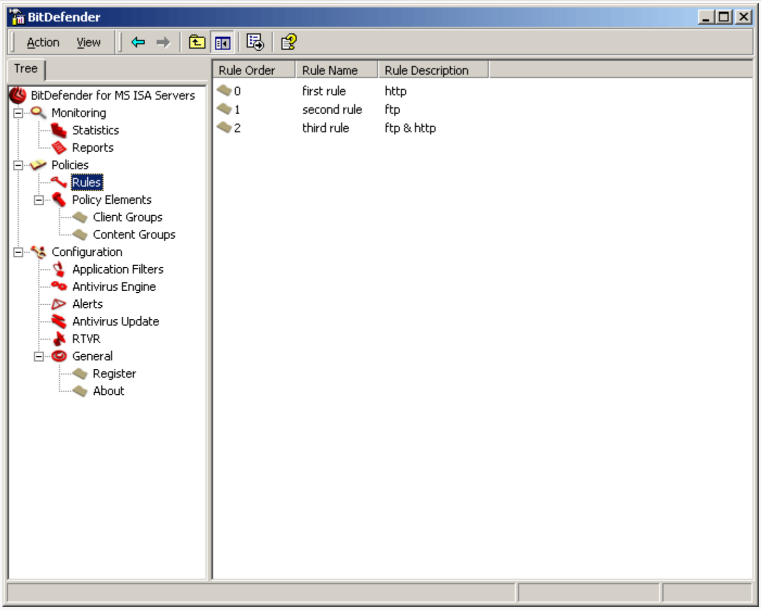
Policies Module

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

- Rules
- Policy Elements

8.1. Rule Creation

Click the **Rules** tab on the management console (**Policies** module). The following window will appear:



Rule Order	Rule Name	Rule Description
0	first rule	http
1	second rule	ftp
2	third rule	ftp & http

Rules

Here you can define specific filtering rules for specific IP address groups across multiple scan types. A system of safe domain white lists configurable by the administrator is also available so that the traffic between the ISA Server and the respective domains is not scanned.

By default BitDefender scans all downloaded files through the HTTP protocol and downloaded & uploaded files through the FTP protocol.

Note

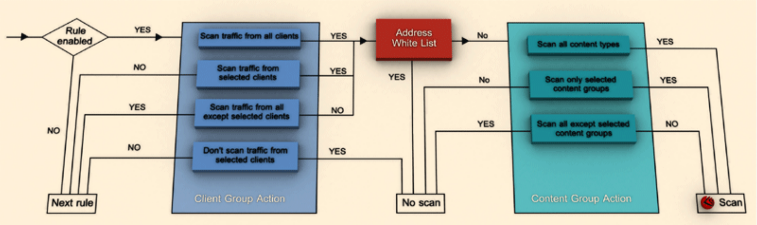
A rule is built for a group of clients.

1. Assignment to a group is done based on the **IP address** of the client having made the request to access the web page or file.
2. Rules are analyzed by order of definition, until the **IP address** is matched to a **Client Group**.
3. The defined action is taken (scan or no scan, depending on the constraints defined in the **Address White List** and the **Content Group**). Then, the IP address leaves the content filter.
4. If no rule is found for the respective IP, the implicit action will be applied: scanning.

It is recommended that one rule be defined for each group as no other newly defined rules will be taken into consideration once a match has been found.

8.1.1. Working Schema

The diagram below shows how the content filter works:


Rule enabled
YES
NO
YES
NO
NO
Next rule
Scan traffic from all clients
Scan traffic from selected clients
Scan traffic from all except selected clients
Don't scan traffic from selected clients
Client Group Action
YES
YES
NO
YES
Address White List
YES
No
No scan
No
YES
Scan all content types
Scan only selected content groups
Scan all except selected content groups
Content Group Action
YES
YES
NO
Scan

Working Schema

If a default rule needs to be defined for any client, it is recommended to choose the last of the rules on the list as it only triggers yes/no answers and the filtering process is finished once the respective client has been checked.

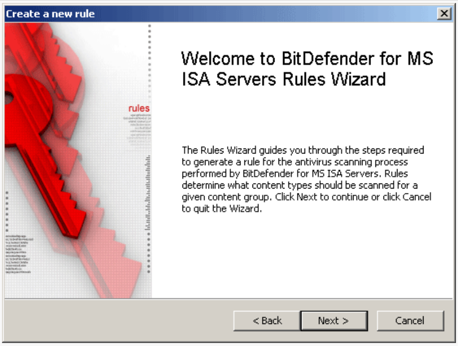
Note

1. You can enable/disable rules by accessing the **Properties** section (double-click the intended rule).
2. The **Client Group Action** is defined under the 4th step of the wizard and you can modify it any time you want by clicking the **Client Group** tab - **Properties** section (double-click the intended rule).
3. The **White List** is defined in the **Protocols** tab - **Properties** section (double-click the intended rule).
4. The **Content Group Action** is defined under the 5th step of the wizard and you can modify it any time you want by clicking the **Content Groups** tab - **Properties** section (double-click the intended rule).

8.1.2. Rules Wizard

To create a rule you must run the **Rules Wizard** (from the contextual menu point **New** and select **Rule**). The wizard is a six step procedure.

Step 1/6 - Welcome to the rules wizard



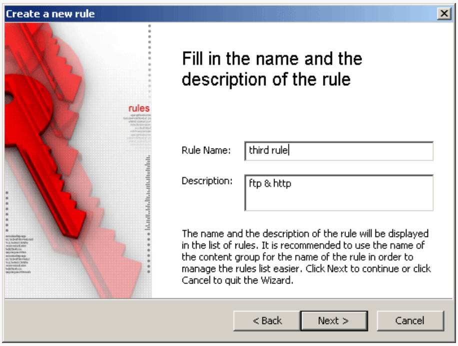
Welcome to BitDefender for MS ISA Servers Rules Wizard

The Rules Wizard guides you through the steps required to generate a rule for the antivirus scanning process performed by BitDefender for MS ISA Servers. Rules determine what content types should be scanned for a given content group. Click Next to continue or click Cancel to quit the Wizard.

Welcome to the rules wizard

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

Step 2/6 - Specify the name and the description of the rule



Fill in the name and the description of the rule

Rule Name: third rule

Description: ftp & http

The name and the description of the rule will be displayed in the list of rules. It is recommended to use the name of the content group for the name of the rule in order to manage the rules list easier. Click Next to continue or click Cancel to quit the Wizard.

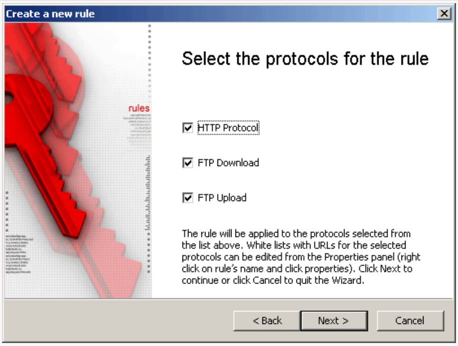
Specify the name and the description of the rule

You must specify the following:

- **Rule Name** - type in a name for the rule;
- **Description** - type in a short description of the rule so that it can be easily identified.

Click **Next**.

Step 3/6 - Select the protocols for the rule



Select the protocols for the rule

☑ HTTP Protocol

☑ FTP Download

☑ FTP Upload

The rule will be applied to the protocols selected from the list above. White lists with URLs for the selected protocols can be edited from the Properties panel (right click on rule's name and click properties). Click Next to continue or click Cancel to quit the Wizard.

Select the protocols for the rule

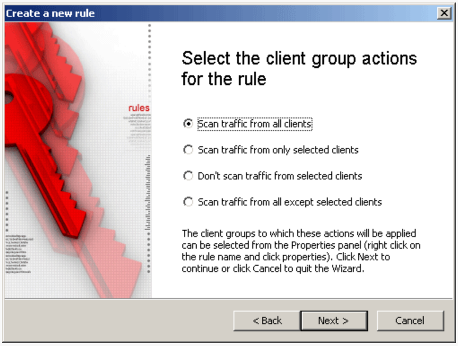
Select the protocols: HTTP, FTP download & upload.

Note

White lists of domains for the selected protocols can be edited by accessing the **Properties** window (double-click the intended rule), **Protocols** tab.

Click **Next**.

Step 4/6 - Select the client group actions



Select the client group actions for the rule

● Scan traffic from all clients

○ Scan traffic from only selected clients

○ Don't scan traffic from selected clients

○ Scan traffic from all except selected clients

The client groups to which these actions will be applied can be selected from the Properties panel (right click on the rule name and click properties). Click Next to continue or click Cancel to quit the Wizard.

Select the client group actions

You must select one of the following client group actions:

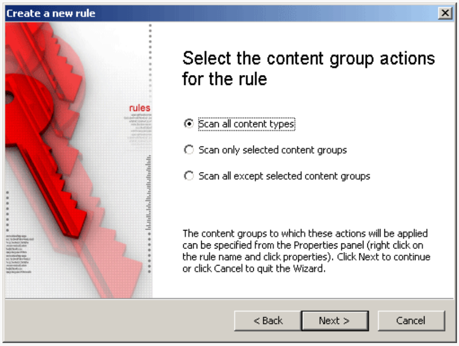
- Scan traffic from all clients.
- Scan traffic from selected clients only.
- Don't scan traffic from selected clients.
- Scan traffic from all except selected clients.

Note

The client groups to which these actions will apply can be edited by accessing the **Properties** window (double-click the intended rule), **Client Groups** tab.

Click **Next**.

Step 5/6 - Select the content group actions



Select the content group actions for the rule

● Scan all content types
○ Scan only selected content groups
○ Scan all except selected content groups

The content groups to which these actions will be applied can be specified from the Properties panel (right click on the rule name and click properties). Click Next to continue or click Cancel to quit the Wizard.

Select the content group actions

You must select one of the following content group actions:

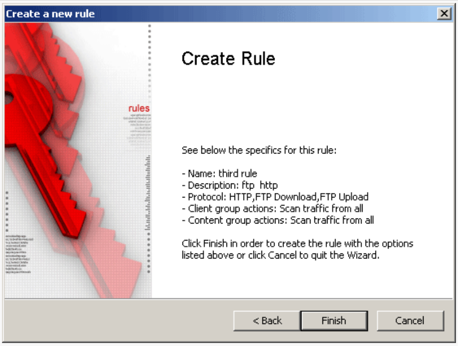
- Scan all content types.
- Scan only selected content groups.
- Scan all except selected content groups.

Note

The content groups to which these actions will be applied can be edited by accessing the **Properties** window (double-click the intended rule), **Content Groups** tab.

Click **Next**.

Step 6/6 - See the summary



Create Rule

See below the specifics for this rule:

- Name: third rule
- Description: ftp http
- Protocol: HTTP,FTP Download,FTP Upload
- Client group actions: Scan traffic from all
- Content group actions: Scan traffic from all

Click Finish in order to create the rule with the options listed above or click Cancel to quit the Wizard.

See the summary

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

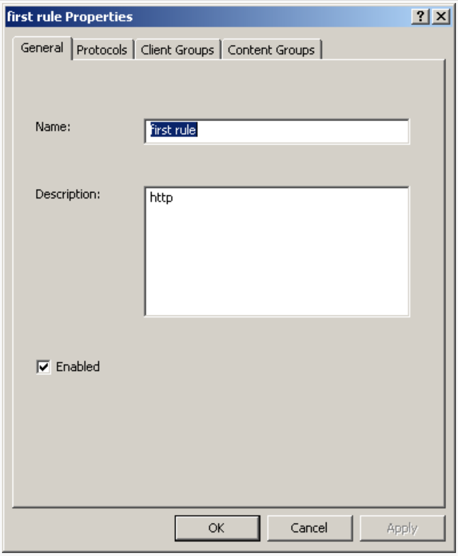
The rule will appear in the Rules section.

8.1.3. Rule Properties

You must access the **Properties** window in order to specify the clients, content types and lists of excluded domains.

Set the general properties

Double-click the intended rule to access the **Properties** window.



Name: first rule

Description: http

☑ Enabled

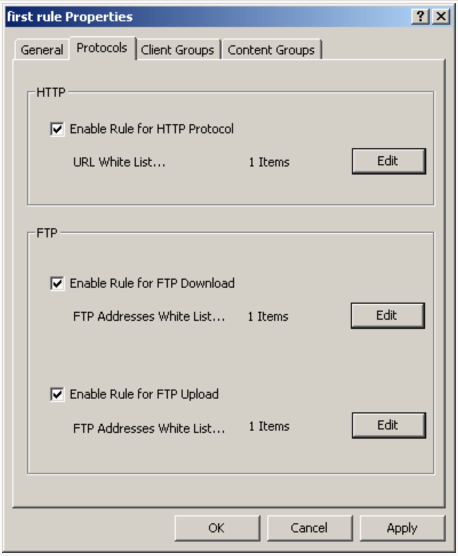
Set the general properties

Here, you can change the name and description of the rule.

Click **Apply** to save the changes.

Configure the domain white lists

Click the **Protocols** tab to access the section where you can configure the domain white lists.


first rule Properties

General | Protocols | Client Groups | Content Groups

HTTP

☑ Enable Rule for HTTP Protocol

URL White List... 1 Items Edit

FTP

☑ Enable Rule for FTP Download

FTP Addresses White List... 1 Items Edit

☑ Enable Rule for FTP Upload

FTP Addresses White List... 1 Items Edit

Configure the domain white lists

It is possible to indicate white lists for the two protocols, HTTP and FTP (upload and download), so that the traffic between the ISA Server and the respective domains will not be scanned.

It is possible to insert a server name in the white list either in full (e.g. `ftp.home.ro`) or partially (`home.ro`), the second choice being the most indicated as certain servers act as an alias for others (e.g. `ftp.home.ro` -> `123.home.ro`).

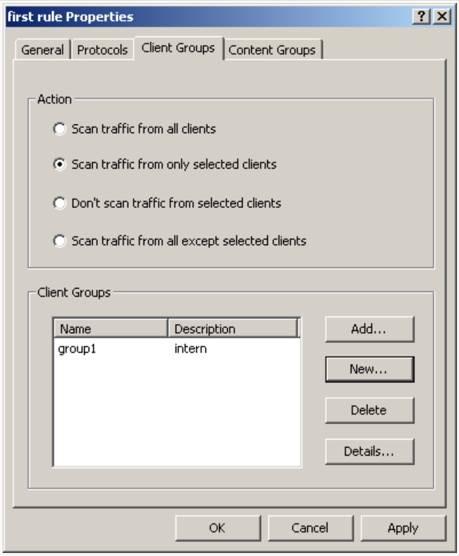
If you want `www.home.ro` to be excepted from scanning, you must add `home.ro` to the **URL White List**.

Click the **Edit** button corresponding to the selected white list and insert the intended domains in the window that appears.

Click **Apply** to save the changes.

Select the client group

Click the **Client Groups** tab to access the section where you can select the client group.



Action

○ Scan traffic from all clients

● Scan traffic from only selected clients

○ Don't scan traffic from selected clients

○ Scan traffic from all except selected clients

Client Groups

Name	Description
group1	intern

Select the client group

Click **Add** and select a previously created group from the Client Groups section. The group will appear in the list. To modify a group select it and click **Details**.

To create a group, click **New** or access the Client Groups section and follow the wizard.

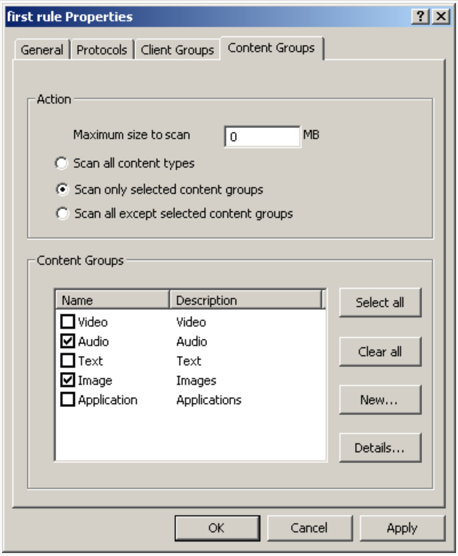
Click **Delete** to delete a group.

You can also change client group actions.

Click **Apply** to save the changes.

Select the content types groups

Click the **Content Groups** tab to access the section where you can select the content types groups.



Action

Maximum size to scan 0 MB

○ Scan all content types

● Scan only selected content groups

○ Scan all except selected content groups

Content Groups

Name	Description
□ Video	Video
☑ Audio	Audio
□ Text	Text
☑ Image	Images
□ Application	Applications

Select the content types groups

In the **Maximum size to scan** field you can specify the maximum size (in MB) of the files that are to be scanned. Thus, if you type in 10, all files larger than 10 MB will be excluded from scanning. If you type in 0 MB, all files will be scanned, regardless of their size.

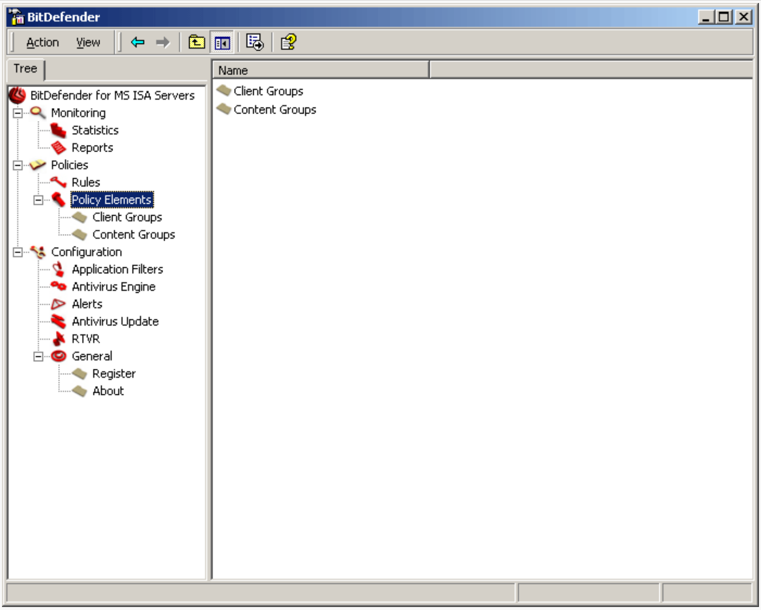
You can see all the previously created groups in the Content Groups section. Select the desired content groups.

To create a group, click Content Groups section and follow the wizard.

Click **Apply** to save the changes and **OK** to return to the Rules section.

8.2. Policy Elements

Click the **Policy Elements** tab on the management console (**Policies** module). The following window will appear:



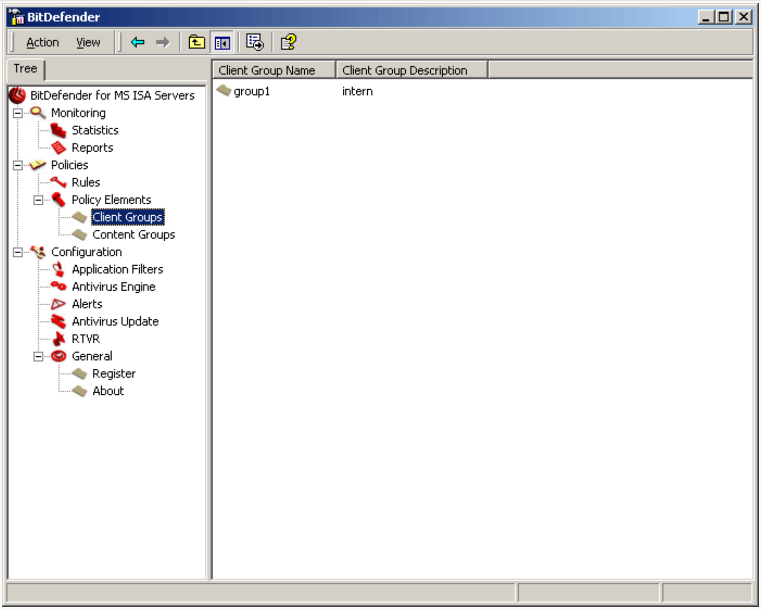
Policy Elements

There are two types of **Policy Elements**:

- **Client Groups**
- **Content Groups**

8.2.1. Client Groups

Click the **Client Groups** tab on the management console (**Policies** -> **Policy Elements** section). The following window will appear:



Client Group Name	Client Group Description
group1	intern

Client Groups

Here you can define custom client groups to be used when creating rules. A group can contain one or more computers.

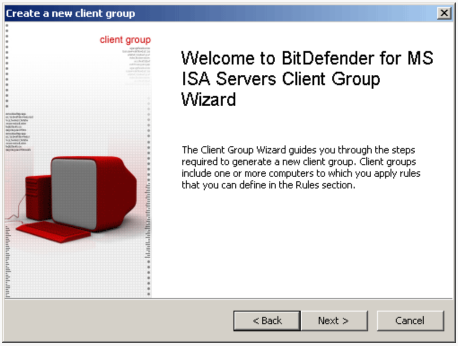
Note

Double-click a group to open the **Properties** window where you can modify its details.

Client Group Wizard

To create a group you must run the **Client Group Wizard** (from the contextual menu point **New** and select **Client Group**). The wizard is a four step procedure.

Step 1/4 - Welcome to the Client Group Wizard



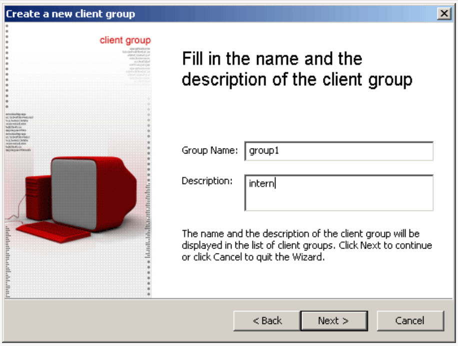
Welcome to BitDefender for MS ISA Servers Client Group Wizard

The Client Group Wizard guides you through the steps required to generate a new client group. Client groups include one or more computers to which you apply rules that you can define in the Rules section.

Welcome to the Client Group Wizard

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

Step 2/4 - Specify the name and the description of the group



Fill in the name and the description of the client group

Group Name: group1

Description: intern

The name and the description of the client group will be displayed in the list of client groups. Click Next to continue or click Cancel to quit the Wizard.

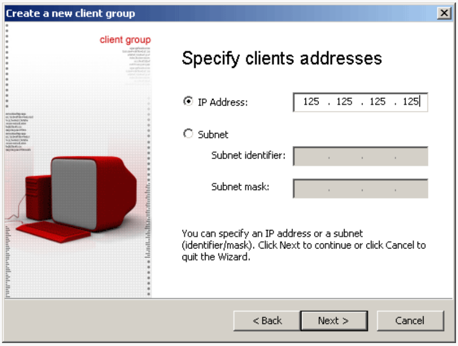
Specify the name and the description of the group

You must specify the following:

- **Group Name** - type in a name for the group;
- **Description** - type in a short description of the group so that it can be easily identified.

Click **Next**.

Step 3/4 - Specify clients addresses



Specify clients addresses

● IP Address: 125 . 125 . 125 . 125

○ Subnet

Subnet identifier:

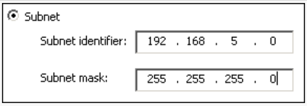
Subnet mask:

You can specify an IP address or a subnet (identifier/mask). Click Next to continue or click Cancel to quit the Wizard.

Specify clients addresses

If your group contains only one computer you must type its ip address in the corresponding field.

For more computers, you must select **Subnet** and type in the identifier and the mask.



● Subnet

Subnet identifier: 192 . 168 . 5 . 0

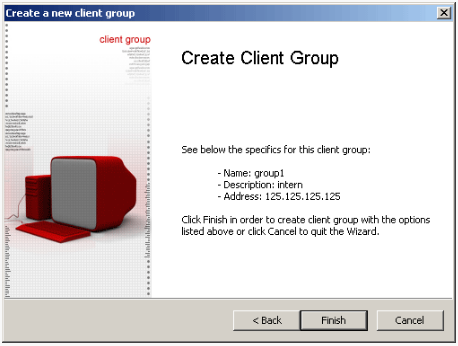
Subnet mask: 255 . 255 . 255 . 0

Subnet

The group will contain all the computers the ip address of which range between 192.168.5.0 and 192.168.5.255.

Click **Next**.

Step 4/4 - See the summary



Create Client Group

See below the specifics for this client group:

- Name: group1
- Description: intern
- Address: 125.125.125.125

Click Finish in order to create client group with the options listed above or click Cancel to quit the Wizard.

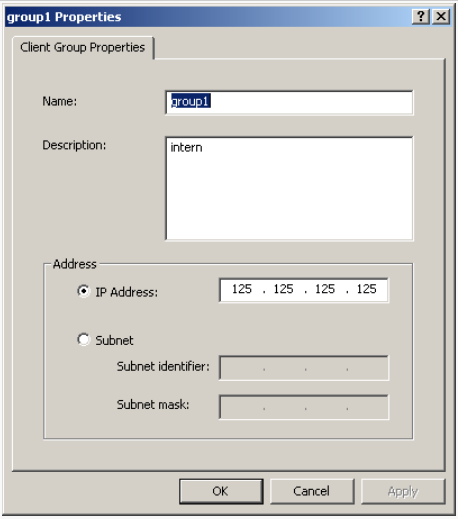
See the summary

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

The group will appear in the Client Groups section.

Client Group Properties

You can modify the details of a group any time you want by double-clicking it. The **Properties** window will appear:



Name: group1

Description: intern

● IP Address: 125 . 125 . 125 . 125

○ Subnet

Subnet identifier: . . .

Subnet mask: . . .

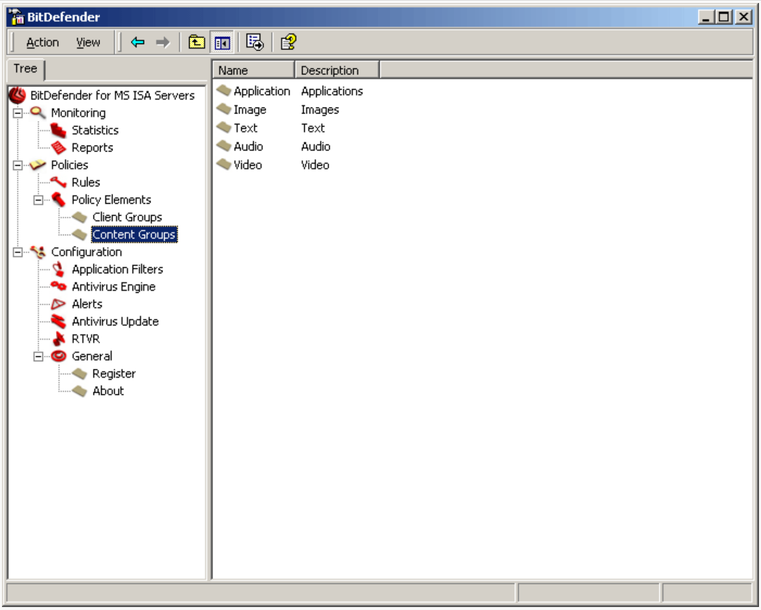
Client Group Properties

Here, you can change the name and description, the ip address or the subnet parameters (identifier and mask) of the group.

Click **Apply** to save the changes and **OK** to return to the Client Groups section.

8.2.2. Content Groups

Click the **Content Groups** tab on the management console (**Policies** -> **Policy Elements** section). The following window will appear:



Name	Description
Application	Applications
Image	Images
Text	Text
Audio	Audio
Video	Video

Content Groups

Here you can define custom content groups to be used when creating rules.

A content group can contain more content types which can be file extensions (.xyz) or MIME types (class/subclass). The second form (MIME types) is only used for the HTTP traffic, when the header is present.

When analyzing an FTP traffic rule, BitDefender will compare the file extension to the extensions defined in the content group. As for the HTTP traffic, if the content-type header is present, its value will be searched in the group content type list. If the content type is not found or the header does not exist, BitDefender will search for the file extension.

By default, BitDefender comes with 5 content groups: **Application**, **Image**, **Text**, **Audio** and **Video**. The default groups are described in the table below:

Default content groups	Description
Application	Contains the following content types: • `application/*` - all the MIME types of the application class are included in this group; • `.vbs, .js, .exe, .com, .dll, .ocx, .scr, .bin, .dat, .386, .vxd, .sys, .wdm, .cla, .class, .ovl, .ole, .hlp, .doc, .dot, .xls, .ppt, .wbk, .wiz, .pot, .ppa, .xla, .xlt, .vbs, .vbe, .mdb, .rtf, .rtf, .htm, .hta, .html, .xml, .xtp, .php, .asp, .js, .shs, .chm, .lnk, .pif, .prc, .url, .smm, .pfd, .msi, .ini, .csc, .cmd, .bas, .nws, .gtar, .gz, .tar, .tgz, .z, .zip` - the files with these extensions are included in this group.
Image	Contains the following content types: • `image/*` - all the MIME types of the image class are included in this group; • `.cod, .cmx, .ief, .pbm, .pnm, .ppm, .gif, .bmp, .jtif, .jpe, .jpg, .jpeg, .ico, .pgm, .ras, .rgb, .dib, .tif, .xbm, .xpm, .xwd` - the files with these extensions are included in this group.
Text	Contains the following content types: • `text/*` - all the MIME types of the text class are included in this group; • `.h, .c, .htc, .vcf, .etx, .uls, .css, .rtx` - the files with these extensions are included in this group.

Default content groups	Description
Audio	Contains the following content types: • `audio/*` - all the MIME types of the audio class are included in this group; • `.ra, .ram, .rmi, .au, .snd, .aif, .aifc, .wav, .m3u, .mid, .mp3` - the files with these extensions are included in this group.
Video	Contains the following content types: • `video/*` - all the MIME types of the video class are included in this group; • `.asf, .asr, .asx, .avi, .ivf, .lsf, .lsx, .mov, .movie, .mlv, .mp2, .mpa, .mpe, .mpg, .mpeg, .mpv2, .qt` - the files with these extensions are included in this group.

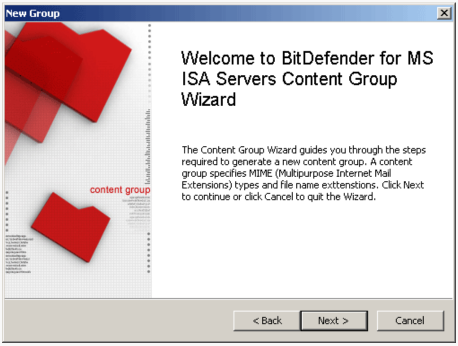
Note

Double-click a group to open the **Properties** window where you can modify its details.

Content Group Wizard

To create a content group you must run the **Content Group Wizard** (from the contextual menu point **New** and select **Content Group**). The wizard is a four step procedure.

Step 1/4 - Welcome to the Content Group Wizard



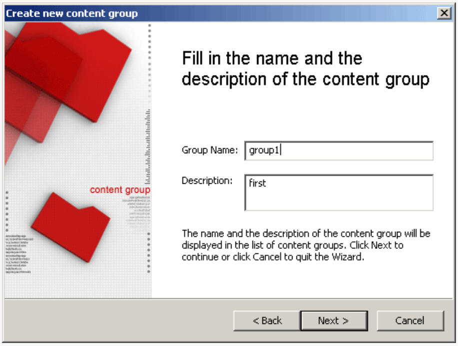
Welcome to BitDefender for MS ISA Servers Content Group Wizard

The Content Group Wizard guides you through the steps required to generate a new content group. A content group specifies MIME (Multipurpose Internet Mail Extensions) types and file name exttenstions. Click Next to continue or click Cancel to quit the Wizard.

Welcome to the Client Group Wizard

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

Step 2/4 - Specify the name and the description of the group



Fill in the name and the description of the content group

Group Name: group1

Description: first

The name and the description of the content group will be displayed in the list of content groups. Click Next to continue or click Cancel to quit the Wizard.

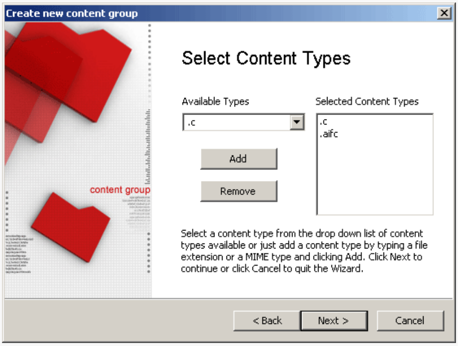
Specify the name and the description of the group

You must specify the following:

- **Group Name** - type in a name for the group;
- **Description** - type in a short description of the group so that it can be easily identified.

Click **Next**.

Step 3/4 - Specify content types



Select Content Types

Selected Content Types

.c
.aifc

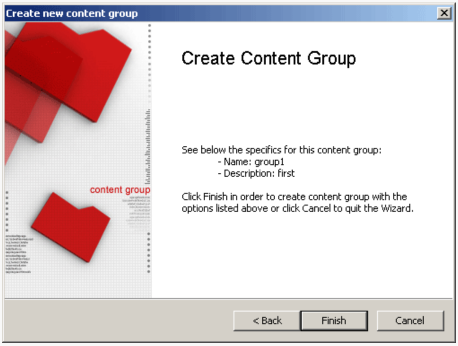
Select a content type from the drop down list of content types available or just add a content type by typing a file extension or a MIME type and clicking Add. Click Next to continue or click Cancel to quit the Wizard.

Specify content types

Select a content type from the drop-down menu or type in a content type and click **Add**. To remove a content type, just select it and click **Remove**.

Click **Next**.

Step 4/4 - See the summary



Create Content Group

See below the specifics for this content group:
- Name: group1
- Description: first

Click Finish in order to create content group with the options listed above or click Cancel to quit the Wizard.

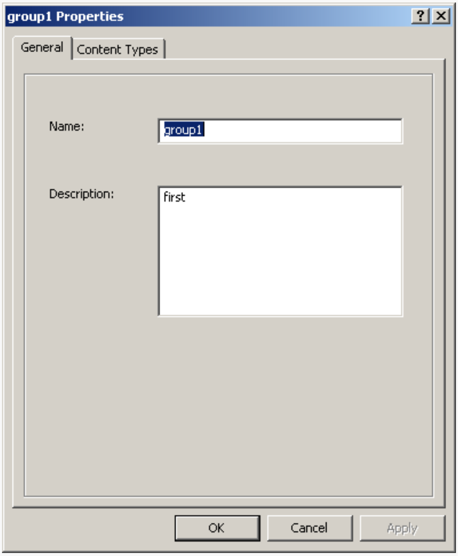
See the summary

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

The rule will appear in the Content Groups section.

Content Group Properties

You can modify the details of a group any time you want by double-clicking it. The **Properties** window will appear:



Name: group1

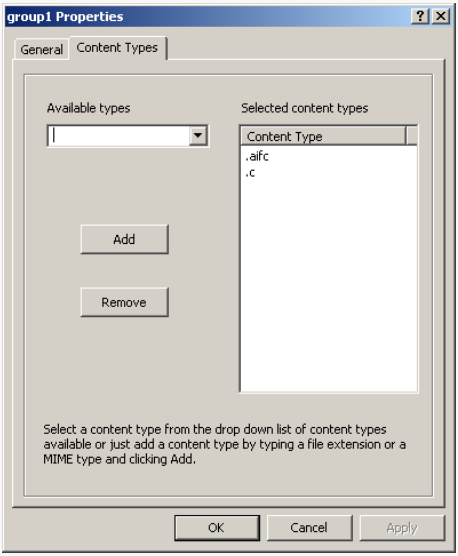
Description: first

Content Group Properties

Here, you can change the name and description.

Click **Apply** to save the changes.

Click the **Content Types** tab if you want to modify the content types.



group1 Properties

General | Content Types

Available types

Selected content types

Content Type

.aifc

.c

Select a content type from the drop down list of content types available or just add a content type by typing a file extension or a MIME type and clicking Add.

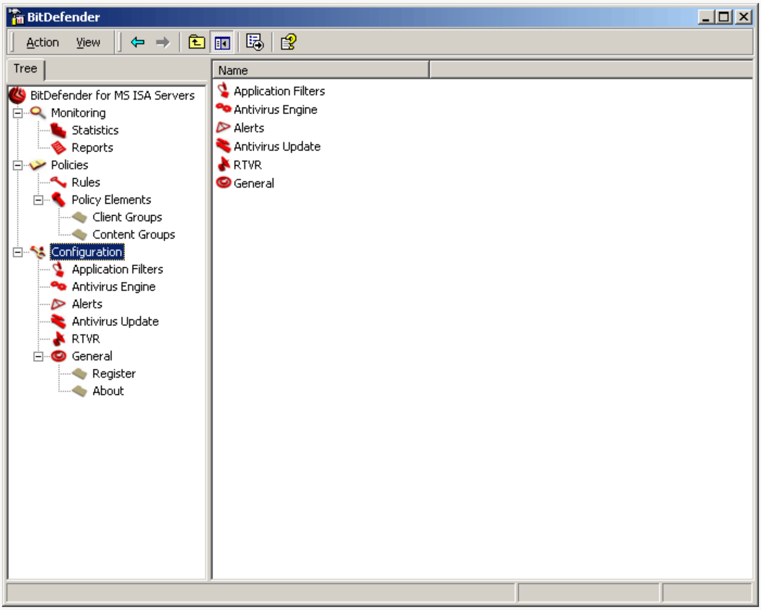
Content Group Properties

You can add a new content type or remove an existing one.

Click **Apply** to save the changes and **OK** to return to the Content Groups section.

9. Configuration Module

Click the **Configuration** tab on the management console. The following window will appear:



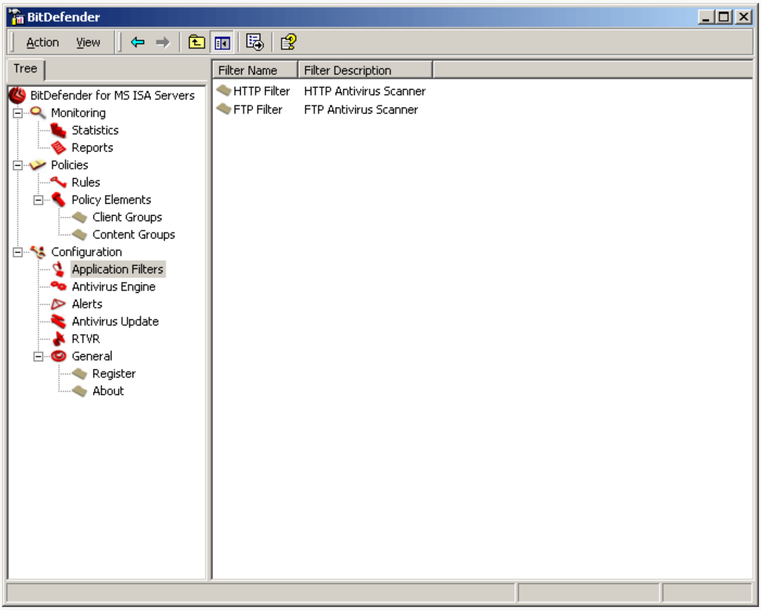
Configuration module

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

- Application Filters
- Antivirus Engine
- Alerts
- Antivirus Update
- RTVR
- General

9.1. Application Filters

Click the **Application Filters** tab on the management console (**Configuration** module). The following window will appear:



Filter Name	Filter Description
HTTP Filter	HTTP Antivirus Scanner
FTP Filter	FTP Antivirus Scanner

Application Filters

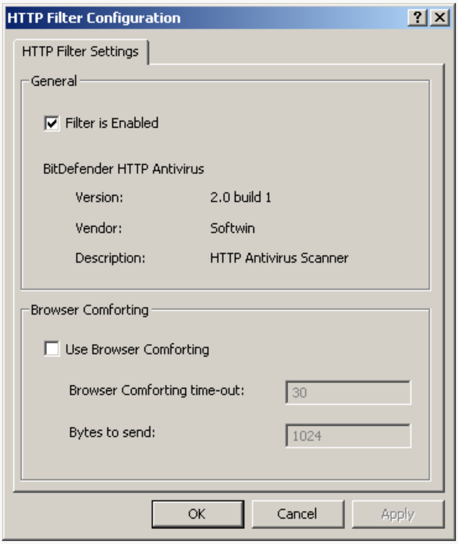
Here you can enable or disable the BitDefender filters that scan all HTTP and FTP-based traffic.

Filter	Description
HTTP	All HTTP responses to clients are sent by the Firewall service of the Microsoft ISA to the BitDefender filter, which decides if they need to be scanned or not. After being scanned, the responses are sent to the clients. The unscanned responses are let through without being intercepted.
FTP	The FTP filter is attached by the Firewall to each FTP session opened by the client. The filter monitors the FTP client-server communication and in case it detects a

Filter	Description
	data connection for file transfer (upload or download), it intercepts such transfer and scans it or not, according to the defined rules.

9.1.1. HTTP Filter

Double-click **HTTP filter**. The following configuration window will appear:



☑ Filter is Enabled

BitDefender HTTP Antivirus

Version: 2.0 build 1

Vendor: Softwin

Description: HTTP Antivirus Scanner

□ Use Browser Comforting

Browser Comforting time-out: 30

Bytes to send: 1024

HTTP Filter Configuration

The window contains 2 sections:

- **General** - keep the **FTP Filter** enabled in order to be protected against viruses and spyware through the HTTP traffic.
- **Browser Comforting** - check the box next to **Use Browser Comforting** if you want to avoid browser time-outs and configure the time-out interval and the number of bytes sent during this interval.

If the **Browser Comforting** option is enabled and a file is downloaded, before such file is scanned, the client could receive small portions of it. If the file is clean all its other parts will be sent to the client. If a virus is detected, the connection will immediately close and no virus alert will appear in the browser.

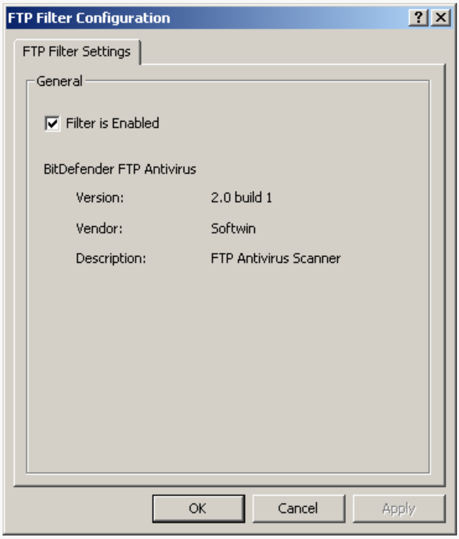
Note

The first portions of the file the client has received may contain the virus, even if in a not active state (the file has the extension of an incomplete download). Such portions must be deleted. That is why it is recommended to use **Browser Comforting** for short periods of time only (for example when you need to download a large file).

Click **Apply** to save the changes and **OK** to return to the Application filters section.

9.1.2. FTP Filter

Double-click **FTP Filter**. The following configuration window will appear:



☑ Filter is Enabled

BitDefender FTP Antivirus

Version: 2.0 build 1

Vendor: Softwin

Description: FTP Antivirus Scanner

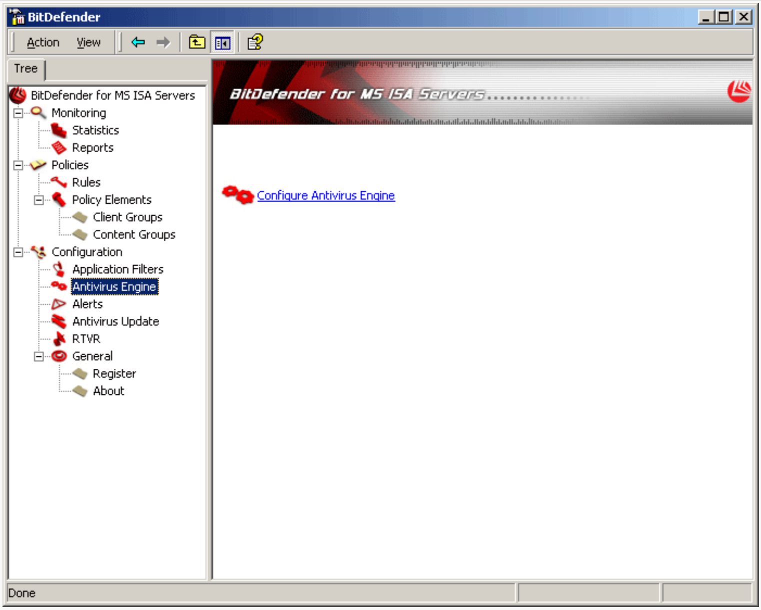
FTP Filter Configuration

Keep the **FTP Filter** enabled in order to be protected against viruses and spyware through the FTP traffic (upload and download).

Click **Apply** to save the changes and **OK** to return to the Application filters section.

9.2. Antivirus Engine

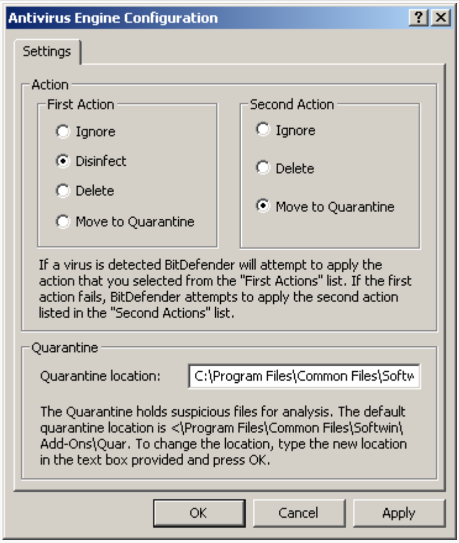
Click the **Antivirus Engine** tab on the management console (**Configuration** module). The following window will appear:



Antivirus Engine

Here you can set the actions to be taken on the infected files and the quarantine location.

Click **Configure Antivirus Engine**. The following window will appear:



Action

First Action

○ Ignore
● Disinfect
○ Delete
○ Move to Quarantine

Second Action

○ Ignore
○ Delete
● Move to Quarantine

If a virus is detected BitDefender will attempt to apply the action that you selected from the "First Actions" list. If the first action fails, BitDefender attempts to apply the second action listed in the "Second Actions" list.

Quarantine

Quarantine location: C:\Program Files\Common Files\Softw

The Quarantine holds suspicious files for analysis. The default quarantine location is <\Program Files\Common Files\Softwin\Add-Ons\Quar. To change the location, type the new location in the text box provided and press OK.

Antivirus Engine Configuration

The window contains 2 sections:

- **Action** - allows for the selection of the BitDefender actions on infected objects.

  BitDefender allows for the selection of two actions to be taken in case an infected document is found.

First action	Description
Ignore	Ignore infected objects. No action taken.
Disinfect	Disinfect infected objects.
Delete	Delete infected objects.
Move to Quarantine	Isolate infected objects in the quarantine zone.

The **Second action** is a supplementary measure of protection and it is only activated if the first action is **Disinfect**.

First action	Description
Ignore	Ignore infected objects. No action taken.
Delete	Delete infected objects.

First action	Description
Move to Quarantine	Isolate infected objects in the quarantine zone.

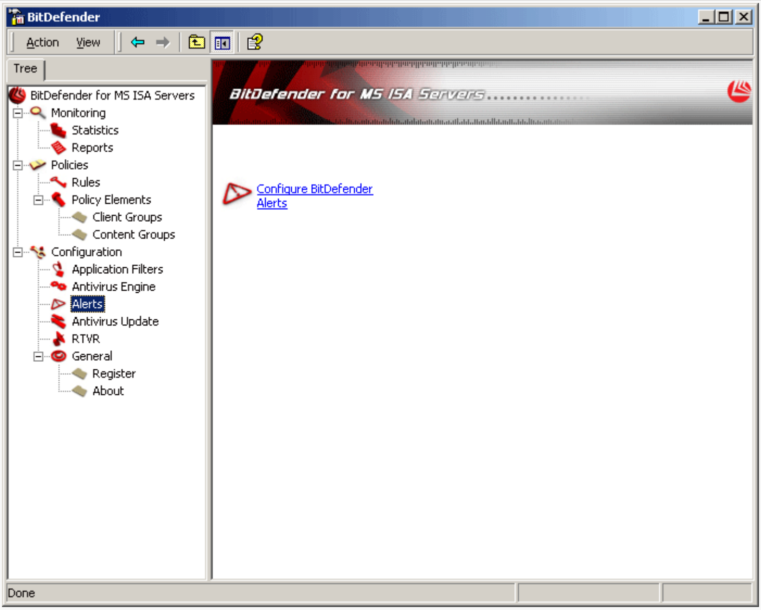
- **Quarantine** - allows for the selection of the quarantine location.

  The default location of the quarantine zone is: `C:\Program Files\Common Files\Softwin\ADD-ONS\quar`. If you want to change it, type the complete path in the **Quarantine location** field (the specified folder must have been previously created).

Click **Apply** to save the changes and **OK** to return to the Antivirus Engine section.

9.3. Alerts

Click the **Alerts** tab on the management console (**Configuration** module). The following window will appear:



Alerts

Here you can configure the alarm messages.

The alert service of Microsoft Internet Security and Acceleration (ISA) Server notifies you when specified events occur. BitDefender has designed 5 special types of events that can generate alarm messages:

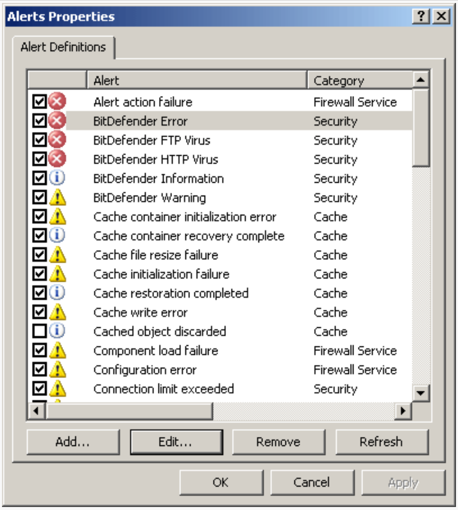
Event	Description
BitDefender Information	An alert is generated when BitDefender services start and stop.
BitDefender Warning	An alert is generated in case a special situation appears: e.g. license expiration (BitDefender will alert you three days in advance), protection disabled, etc.
BitDefender Error	An alert is generated upon the occurrence of a malfunction of BitDefender. Such situations may appear, for example, because of the accidental deletion of some files or of the failure to load the Antivirus engines.
BitDefender HTTP Virus	An alert is generated in case an infected file is detected in the HTTP traffic.
BitDefender FTP Virus	An alert is generated in case an infected file is detected in the FTP traffic.

Click **Configure BitDefender Alerts** to access the **Alerts** section from the Microsoft ISA user interface.

Note

You can also see if the BitDefender plug-ins are initiated (**BitDefender Information** alerts: one for the HTTP filter and the other one for the FTP filter).

Click **Configure Alert Definitions** on the right side panel. The following window will appear:



	Alert	Category
☑ ⊗	Alert action failure	Firewall Service
☑ ⊗	BitDefender Error	Security
☑ ⊗	BitDefender FTP Virus	Security
☑ ⊗	BitDefender HTTP Virus	Security
☑ ⓘ	BitDefender Information	Security
☑ ⚠	BitDefender Warning	Security
☑ ⚠	Cache container initialization error	Cache
☑ ⓘ	Cache container recovery complete	Cache
☑ ⚠	Cache file resize failure	Cache
☑ ⚠	Cache initialization failure	Cache
☑ ⓘ	Cache restoration completed	Cache
☑ ⚠	Cache write error	Cache
□ ⓘ	Cached object discarded	Cache
☑ ⚠	Component load failure	Firewall Service
☑ ⚠	Configuration error	Firewall Service
☑ ⚠	Connection limit exceeded	Security

Alerts Properties

You can set one or more of the following actions to be performed when an alert condition is met:

- Send an e-mail message.
- Take specific action.
- Record the event in the Windows event log - this is done by default for all BitDefender events.
- Stop or start any ISA Server service.

If you want to be notified when an alert is generated you must select the event, click **Edit** (or double-click it), click the **Actions** tab and check the box next to **Send e-mail**. You must fill in the following fields:

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

Note

It is necessary to type in 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.

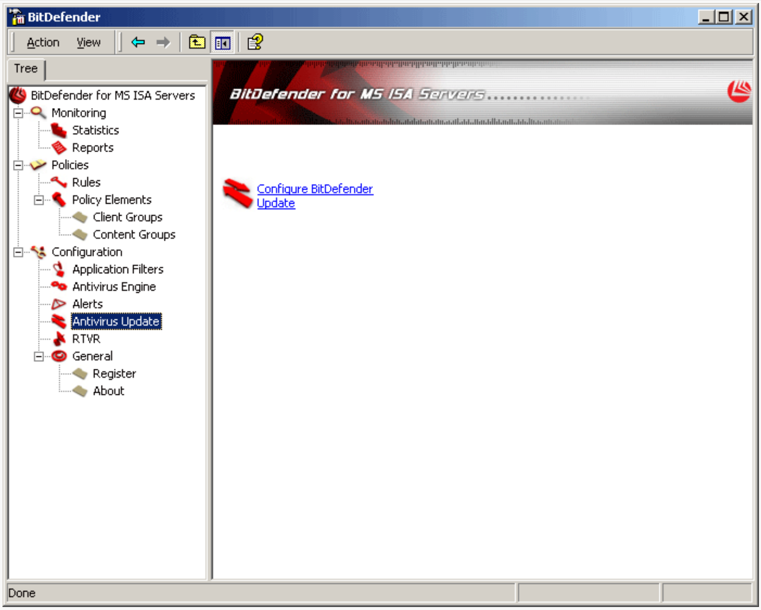
- **To** - type in the e-mail address to which the alert will be sent;

- **Cc** - type in the carbon copy e-mail address.

Click **Apply** to save the changes and **OK** to return to the Alerts section.

9.4. Antivirus Update

Click the **Antivirus Update** tab on the management console (**Configuration** module). The following window will appear:



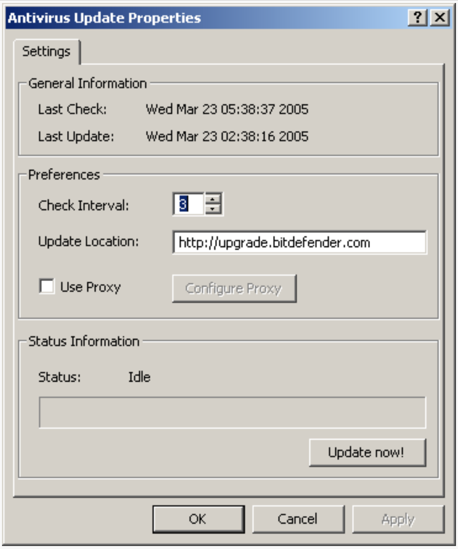
Antivirus Update

Here you can configure the BitDefender update settings.

Nowadays the risk of having your computer infected is higher both because of the appearance of new viruses and spyware and of the spread of existing ones. **BitDefender for MS ISA Servers Enterprise Edition** has a built-in function for the automatic update of virus definitions.

Every 3 hours the update function is launched and it connects to the BitDefender upgrade server. In case an update is found, such update is done transparently, without administrator's intervention, through a file download.

Click **Configure BitDefender Update**. The following window will appear:



Antivirus Update Properties

Settings

General Information

Last Check: Wed Mar 23 05:38:37 2005

Last Update: Wed Mar 23 02:38:16 2005

Preferences

Check Interval: 3

Update Location: http://upgrade.bitdefender.com

□ Use Proxy

Status Information

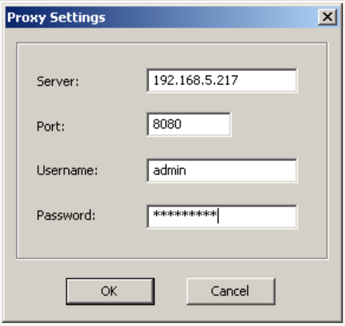
Status: Idle

Antivirus Update Properties

The window contains 3 sections:

- **General information** - contains the date and time of the last check and update.
- **Preferences** - allows for the selection of the update options. By default, the check interval is 3 hours. If you want to change it, type a new interval in the **Check interval** field. If you want to modify the update location, type the name of a new location in the **Update location** field, then click **Apply**.

  If you are using a proxy server with authentication to access the Internet, check the box next to **Use proxy** and click **Configure Proxy**. The following window will appear:


Proxy Settings

Server: 192.168.5.217

Port: 8080

Username: admin

Password: *********

Proxy Settings

You must fill the following fields in with the required information:

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

Note

You might also need to type in the domain name in order to authenticate. Instead of the user name, you can fill the field in with `domain\user` information.

Click **OK** to save the changes.

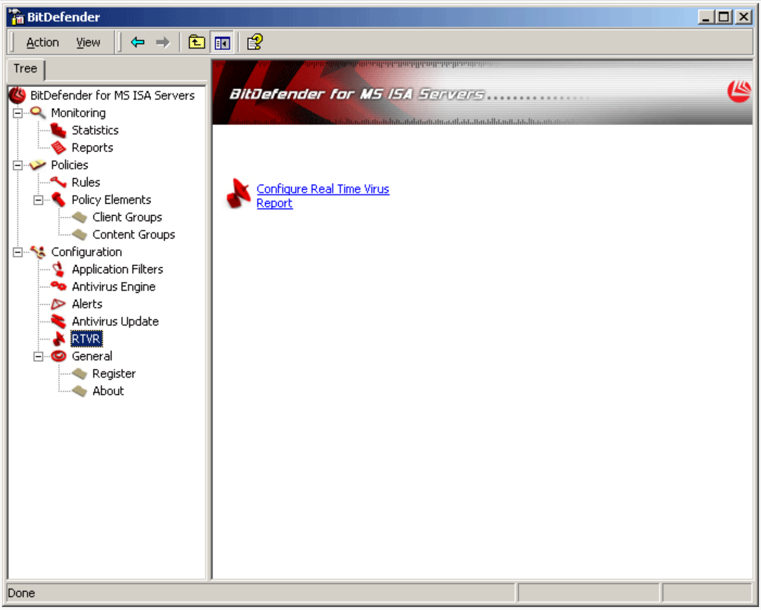
- **Status information** - shows the status of the update process.

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

Click **Apply** to save the changes and **OK** to return to the Antivirus Update section.

9.5. Real Time Virus Report

Click the **RTVR** tab on the management console (**Configuration** module). The following window will appear:



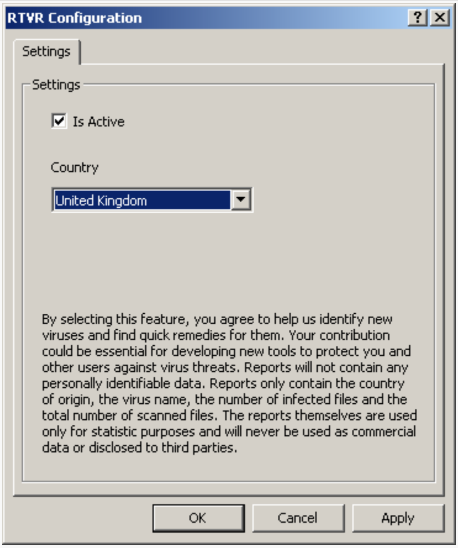
RTVR

Here you can enable the virus reporting feature.

The module is customized for each country and it allows for the sending of alerts on found viruses to the BitDefender Lab. The reports will contain no confidential data, such as your name, IP address or other, and they will not be used for commercial purposes.

The information supplied will only include the name of the country and the virus name and it will solely be used to create statistic reports.

Click **Configure Real Time Virus Report**. The following window will appear:



Settings

☑ Is Active

Country: United Kingdom

By selecting this feature, you agree 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. Reports will not contain any personally identifiable data. Reports only contain the country of origin, 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.

RTVR Configuration

From the scroll-down list, select the country you live in. Check the box next to **Is Active** to enable **RTVR**.

Note

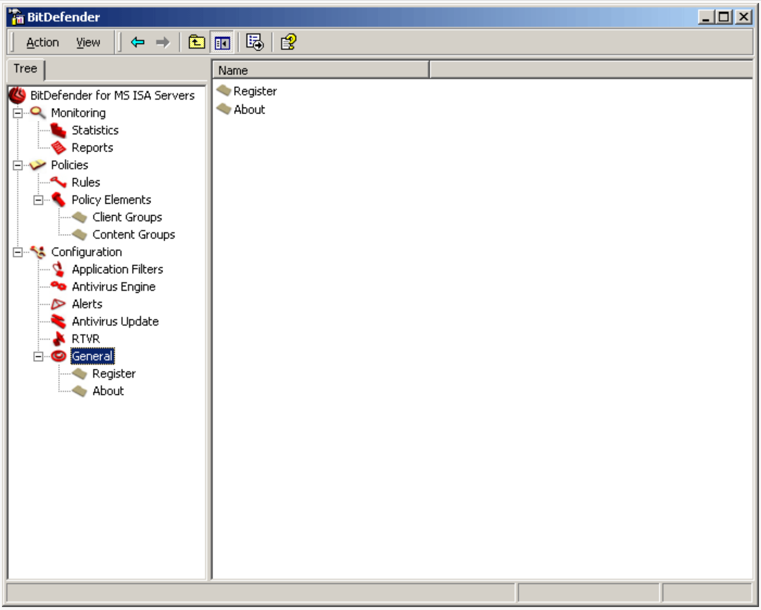
To stop the virus reporting, clear the box next to **Is Active**.

Click **Apply** to save the changes and **OK** to return to the RTVR section.

To see the statistic reports on virus activity, follow the link: http://www.bitdefender.com/bd/site/virusinfo.php?menu_id=2&dc=1&source=2.

9.6. General Information

Click the **General** tab on the management console (**Configuration** module). The following window will appear:

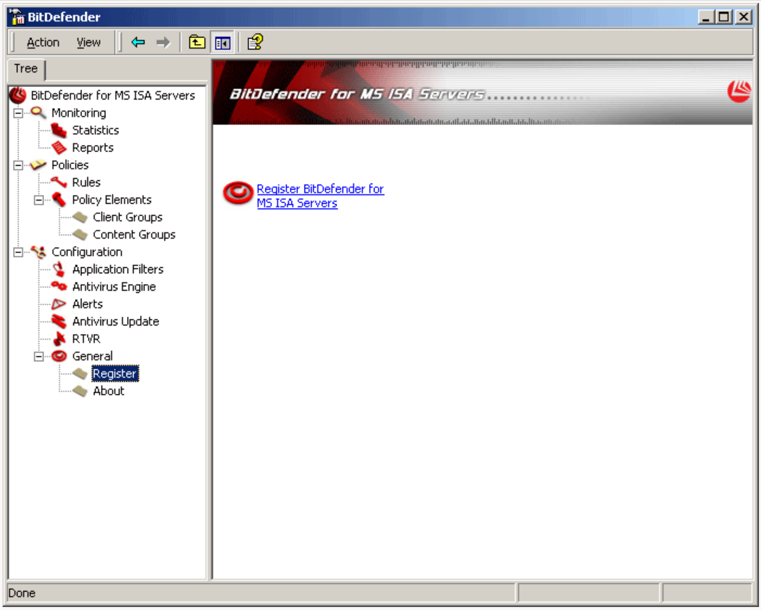


General Information

Click **Register** to check the status of your BitDefender license or **About** to see general information about the product.

9.6.1. Product Registration

To modify the default serial number, click the **Register** tab on the management console (**Configuration -> General** section). The following window will appear:

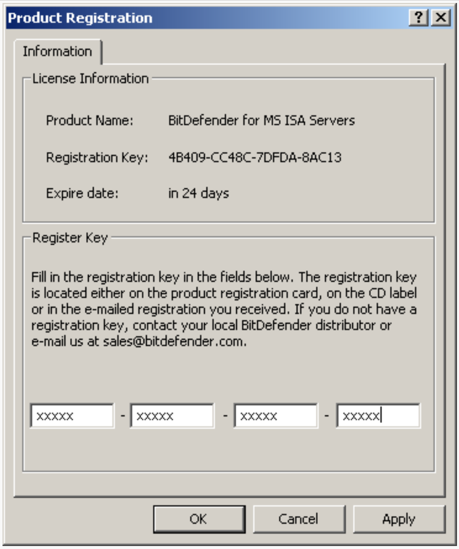


Register

Here you can register the product and you can see the expiring date.

The product is delivered with a trial registration key valid for thirty days. At the end of the trial period, if you want to purchase the product you must provide a new serial number.

Click **Register BitDefender for MS ISA Servers**. The following window will appear:



License Information

Product Name: BitDefender for MS ISA Servers

Registration Key: 4B409-CC48C-7DFDA-8AC13

Expire date: in 24 days

Register Key

Fill in the registration key in the fields below. The registration key is located either on the product registration card, on the CD label or in the e-mailed registration you received. If you do not have a registration key, contact your local BitDefender distributor or e-mail us at sales@bitdefender.com.

xxxxx - xxxxx - xxxxx - xxxxx

Product Registration

Type the new license key in the corresponding fields.

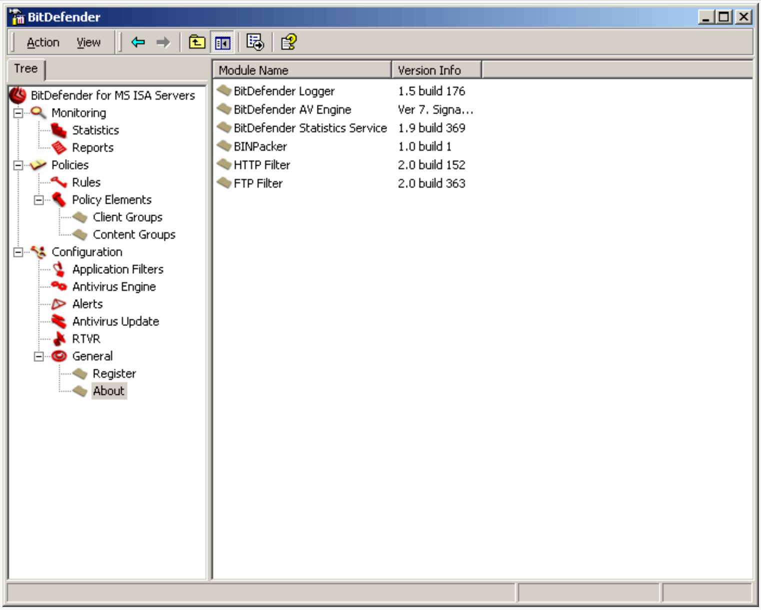
Note

The registration key is to be found either on the product registration card, on the CD label or in the registration e-mail you have received. If you do not have a registration key, contact your local BitDefender distributor or e-mail us at sales@bitdefender.com.

Click **Apply** to save changes and **OK** to return to the Register section.

9.6.2. Product Information

Click the **About** tab on the management console (**Configuration -> General** section). The following window will appear:



Module Name	Version Info
BitDefender Logger	1.5 build 176
BitDefender AV Engine	Ver 7. Signa...
BitDefender Statistics Service	1.9 build 369
BINPacker	1.0 build 1
HTTP Filter	2.0 build 152
FTP Filter	2.0 build 363

Register

Here you can see the current version of the product.

Best Practices

10. Best Practices

Steps to follow in order to make sure you are free from viruses&spyware:

1. **Check whether the BitDefender plug-ins are active.** Once the installation process is over, access the Microsoft ISA user interface and check whether the BitDefender plug-ins (**BitDefender Filter** and **BitDefender Antivirus Filter**) are active in the **Configuration -> Add-ins -> Application Filters** and **Web Filters** sections.
2. **Check whether the FTP rules are active.** If you have previously created a rule for the FTP protocol, check whether the **BitDefender Filter** and the **FTP Access Filter** are enabled (double-click the rule, click the **Protocols** tab, select **FTP**, click **Edit**, click the **Parameters** tab and check the boxes next to each such parameter).
3. **Check whether the BitDefender plug-ins are initiated.** Check whether the BitDefender plug-ins are initiated in the **Monitoring -> Alerts** section (**BitDefender Information** alerts: one for the HTTP filter and the other one for the FTP filter). Click **Configure Alerts Definition** to configure the alerts. To modify an alert select it and click **Edit**. All alerts are active by default.
4. **Access the BitDefender Management Console.** Open the **BitDefender Management Console** by following the path: **Start -> Programs -> BitDefender for MS ISA Servers -> BitDefender for MS ISA Servers**.
5. **Register BitDefender.** Access the Register section (**Configuration -> General -> Register**), click **Register BitDefender for MS ISA Servers**, type in the serial number and click **Apply&OK**.
6. **Configure the update.** Access the Antivirus Update section (**Configuration -> Antivirus Update**), click **Configure BitDefender Update** and, if you are using a proxy, select **Use Proxy**, click **Configure Proxy** and type in the setting.
7. **Select the action to be taken on infected objects.** Access the Antivirus Engine section (**Configuration -> Antivirus Engine**), click **Configure Antivirus Engine** and select the desired action: Disinfect, Delete, Move to Quarantine or Ignore (no action).

   Note

   For **Disinfect** you can select a second action in case the disinfection fails.

8. **Use the EICAR test to check whether BitDefender is working.** Download the Eicar file from www.eicar.org/anti_virus_test_file.htm. If your browser displays the **Download Blocked** message then the HTTP Filter is properly configured and

working. Access the Statistics section (**Monitoring -> Statistics**) and check the number of infected files.

9. **Create policy rules.** Five content groups (Video, Audio, Text, Image and Application) are defined in the Rules section (**Policies -> Rules**) and they can be used to create rules for the HTTP&FTP traffic. By default, BitDefender scans all the HTTP traffic, FTP upload & download, irrespective of the client address or of the content type. You can add rules or modify the ones you have already created. BitDefender will decide if a file is scanned or not after the rules are analyzed by order of priority (0 meaning the maximum priority). When a rule dictates that a file is to be scanned or not, the action is executed and the other rules are no longer analyzed. If all the rules have been analyzed and no action has been decided upon the file will be scanned.

10. **Browser Comforting option.** To avoid browser timeouts, you may enable the **Browser Comforting** option, from the Application Filters section (**Configuration -> Application Filters -> HTTP Filter**) and configure the time-out interval and the number of bytes sent during this interval. If the **Browser Comforting** option is enabled and a file is downloaded, the client could receive small portions of the file before it is scanned. If the file is clean, all its other parts will be sent to the client. If a virus is detected, the connection will immediately close and no virus alert will appear in the browser.

    Note

    The first portions of the file the client has received may contain the virus, even if in a not active state (the file has the extension of an incomplete download). Such portions must be deleted. That is why it is recommended to use **Browser Comforting** for short periods of time only (for example when you need to download a large file).

11. **Configure the alerts.** If a virus is detected, Microsoft ISA Server offers you the option to send mail notification by configuring the BitDefender alerts from the **Monitoring** section on the Microsoft ISA user interface.

    Note

    For more details access the Alerts section of this user guide.

12. **View the statistics.** You can check the antivirus activity in the Statistics section (**Monitoring -> Statistics**).

13. **Create report files.** From time to time, create report files on the antivirus activity in the Reports section (**Monitoring -> Reports**).

BitDefender Enterprise Manager Integration

11. Why BitDefender Enterprise Manager?

BitDefender Enterprise Manager is a scalable, superior solution for 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.

11.1. BitDefender Enterprise Manager Integration Advantages

BitDefender for MS ISA Servers Enterprise Edition deeply integrates with BitDefender Enterprise Manager, which means that you can configure this product from the Enterprise Management Console.

The additional BitDefender for MS ISA Servers Enterprise Edition task templates from the BitDefender Enterprise Manager interface offer several benefits and advantages:

Configure BitDefender for MS ISA Servers Enterprise Edition.

- Allows for the configuration of all BitDefender for MS ISA Servers Enterprise Edition settings in a single step.
- Ensures a uniform BitDefender configuration, according to the pre-established internal policy, by running the task on all BitDefender for MS ISA Servers Enterprise Edition clients.
- Offers the possibility of passing the product management task from the local admin of the ISA Server on to the admin of the BitDefender for MS ISA Servers Enterprise Edition
- Does not require any additional rights when remotely configuring BitDefender for MS ISA Servers Enterprise Edition. Consequently, no modification of the internal right policy is necessary.

Get BitDefender Status.

- Offers a list of the entire configuration of the BitDefender for MS ISA Servers Enterprise Edition 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 for MS ISA Servers Enterprise Edition clients, by generating reports based on the results of this task. The report can be generated periodically, printed or exported in HTML format for further information processing.

Get BitDefender for MS ISA Servers Enterprise Edition Statistics.

- Offers general or specific information about the activity of the BitDefender for MS ISA Servers Enterprise Edition 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 the BitDefender for MS ISA Servers Enterprise Edition clients, by generating reports based on the results of this task. The report 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 MS ISA Servers Enterprise Edition products in the organization.
- Offers the possibility of passing the product activity monitoring task from the local admin of the ISA Server on to the admin of BitDefender for MS ISA Servers Enterprise Edition.

12. Description and Features

BitDefender Enterprise Manager allows for the full automation of routine tasks (including upgrades and updates), while allowing 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). These tasks can be executed across the BitDefender Enterprise Manager network. The WMI server add-on is available with Enterprise 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.

12.1. 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

12.2. 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.

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

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.

Remote Management. Management is available from any network connected system, drastically reducing incident response time.

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.

12.3. The Architecture

BitDefender Enterprise Manager is divided into several parts: BitDefender Server, BitDefender Local Manager, BitDefender Management Console, BitDefender Deployment Tool and BitDefender Update Server.

12.3.1. BitDefender Server

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

- install/uninstall the antivirus product;
- antivirus scanning;
- scheduled scanning;
- update virus definitions database;
- remotely change the security options of the BitDefender products installed on workstations;
- generate detailed reports and statistics.

This component can be considered the "brain" of the product. The tasks received from the user through the management console are forwarded to the workstations in order to be executed, while the information received from the workstations is processed by the server. The information is then forwarded to the management console where it can be viewed and interpreted by the administrator. The server can be dynamically extended to perform various other security-related tasks that the customers may need. The server can be password protected. The password can be set in the management console.

12.3.2. BitDefender Local Manager

This component is installed on each workstation which the administrator may want to administer through BitDefender Enterprise Manager. Through this component, the BitDefender Server communicates with the workstations within the network and it assigns different tasks to the BitDefender products installed on them. This component maintains a local database containing information on each BitDefender product installed on that workstation.

12.3.3. BitDefender Management Console

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

- Easily administer the workstations, by organizing them into workgroups;
- Remotely install the BitDefender products;
- Assign new tasks to the BitDefender products installed on workstations;
- Set the tasks so that they may be executed on one workstation only, on groups or on all workstations within the network;

- Schedule tasks, such as: scanning, virus definitions update and protection options configuration;
- Display alerts that are generated when tasks fail (in order to find the source of these errors), when suspect / infected files are found on workstations or whenever an error occurs;
- Create and display different reports and statistics.

12.3.4. BitDefender Deployment Tool

This is a independent component. It allows for the remote installation of the **BitDefender Local Manager**, supplanting the need to locally install it on each workstation. However, on some operating systems (Microsoft Windows 98, Windows ME) this local installation is a necessity. In case the remote installation fails, you can create an unattended package that you will have to run on the target computers.

12.3.5. BitDefender Update Server

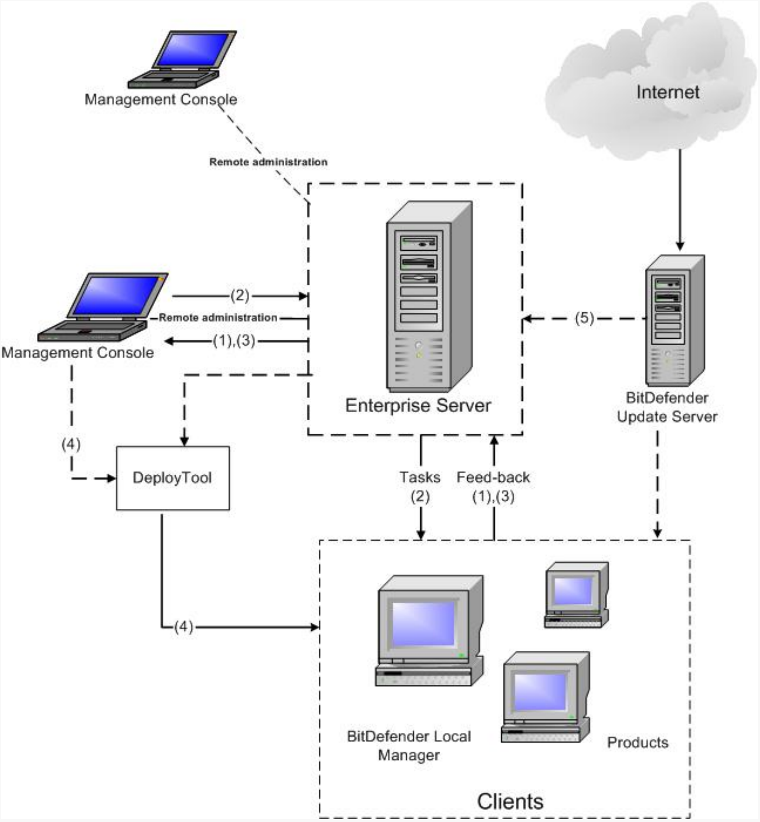
This component allows you to set up an upgrade location within your local network. This way you needn't worry about updating the products installed on computers that are not connected to the Internet, achieving, at the same time, faster updates and reduced Internet traffic. The **BitDefender Update Server** is easy to configure through an intuitive step by step wizard. It will help you get the latest updates for all BitDefender products.

Note

The only components visible to the user are the **BitDefender Management Console**, **BitDefender Deployment Tool** and **BitDefender Update Server**.

12.4. Operation Diagram

The design below shows how **BitDefender Enterprise Manager** works:



Operation Diagram

BitDefender Enterprise Manager is divided into several parts: BitDefender Server, BitDefender Local Manager, BitDefender Management Console, BitDefender Deployment Tool and BitDefender Update Server.

As shown in the diagram above, there are five information flows which can be described as follows:

1. **BitDefender Deployment Tool** sends the task of installing **BitDefender Local Manager** to the workstations.
2. **BitDefender Local Manager** creates a database of all the BitDefender products already installed on the workstations and then sends the information to the

BitDefender Server. The Server takes it over and sends it to the **BitDefender Management Console**, where the user can access it.

3. The user selects the protection options for all BitDefender products through the management console. These options are received by the **BitDefender Server** and they are forwarded to the **BitDefender Local Manager** corresponding to each workstation. Further on, BitDefender products will execute the commands selected by the user through the management console.
4. The results of the command execution at workstation level are sent to the **BitDefender Server**. Depending on the user's option, this information is used to create reports that can be viewed through the management console.
5. **BitDefender Update Server** sets up an upgrade location within your local network, in a folder that must be published in order to make the updates available to the network clients. Next, the administrator can create update tasks from this location using the **BitDefender Management Console**. Client workstation users can also choose to update their antivirus product from this location.

Note

You can publish the download folder by using the **BitDefender HTTP Server** or another HTTP server such as IIS or Apache.

13. Supported Clients

BitDefender Enterprise Manager smoothly integrates with and manages:

Workstation Clients

- **BitDefender Client Professional Plus v8**
- **BitDefender Client Standard v8**
- **BitDefender Standard Edition v7.2 (Server Add-On)**
- **BitDefender Professional Edition v7.2 (Server Add-On)**
- **BitDefender WMI Scripts v1.1 (Server Add-On)**

Server Products

- **BitDefender for Mail Servers (Win SMTP) v1.9**
- **BitDefender for File Servers v1.9, v2.0**
- **BitDefender v2.0 for MS ISA**
- **BitDefender v1.9 for Exchange 5.5**
- **BitDefender v1.9 for Exchange 2000**
- **BitDefender v1.9 for Exchange 2003**
- **BitDefender AntiSpam for Mail Servers (Win SMTP Proxy)**

14. Additional Task Templates

BitDefender for MS ISA Servers Enterprise Edition deeply integrates with BitDefender Enterprise Manager, meaning you can configure this product from the Enterprise Management Console.

Note

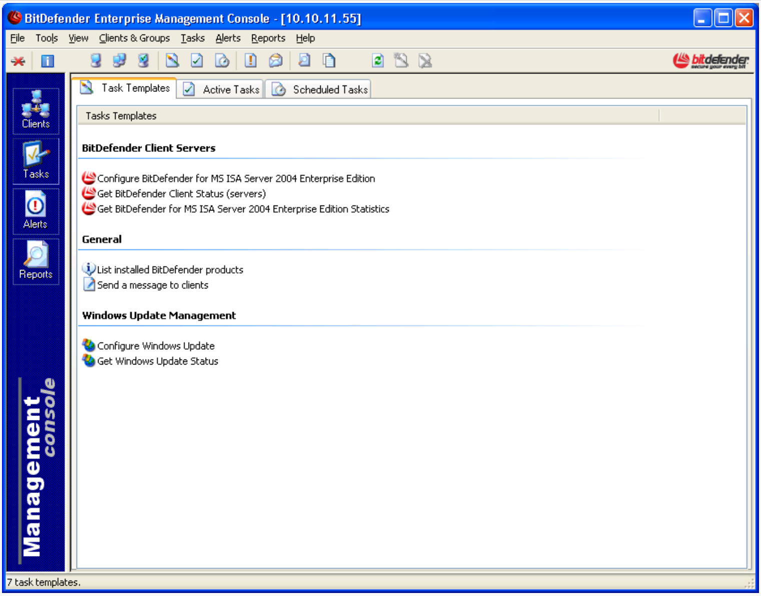
The **BitDefender for MS ISA Servers Enterprise Edition** must be installed on a BitDefender Enterprise client. This means the **BitDefender Local Manager** is already installed on that workstation or it will be installed in order to import the newly created tasks from that workstation.

Open the **BitDefender Enterprise Management Console** by following the path **Start -> Programs -> BitDefender Enterprise Manager -> BitDefender Management Console**.

Access the **Clients** section, select the client that has **BitDefender for MS ISA Servers Enterprise Edition** installed and from the **Clients&Groups** menu, point **Clients**, click **Import Tasks Templates from Selected Clients**.

The imported task templates will become visible in the **Tasks Templates** section. To access it, do any of the following:

- Click **Task Templates** 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 shortcut **CTRL+4**.


BitDefender Enterprise Management Console - [10.10.11.55]
File Tools View Clients & Groups Tasks Alerts Reports Help
bitdefender
Clients
Tasks
Alerts
Reports
Management console
Task Templates
Active Tasks
Scheduled Tasks
Tasks Templates

BitDefender Client Servers

- Configure BitDefender for MS ISA Server 2004 Enterprise Edition
- Get BitDefender Client Status (servers)
- Get BitDefender for MS ISA Server 2004 Enterprise Edition Statistics

General

- List installed BitDefender products
- Send a message to clients

Windows Update Management

- Configure Windows Update
- Get Windows Update Status

7 task templates.

Additional Task Templates

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

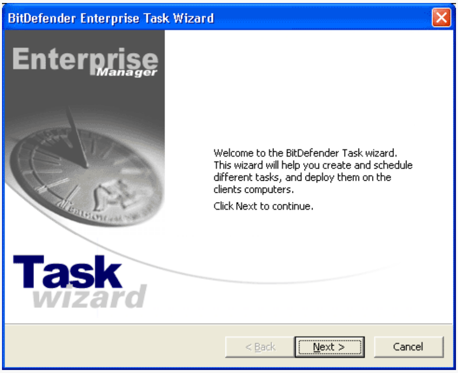
- Configure BitDefender for MS ISA Servers Enterprise Edition - to configure BitDefender for MS ISA Servers Enterprise Edition
- Get BitDefender Client Status (servers) - to receive information about the antivirus status.
- Get BitDefender for MS ISA Servers Enterprise Edition Statistics - to receive statistics about the antivirus product.

14.1. Configure BitDefender for MS ISA Servers Enterprise Edition

In order to configure **BitDefender for MS ISA Servers Enterprise Edition** on one or more servers, double-click the **Configure BitDefender for MS ISA Servers**

Enterprise Edition icon (from the **Task Templates** pane). This will launch the wizard, which will guide you through the process:

14.1.1. Step 1/5 - Welcome to the BitDefender Task Wizard



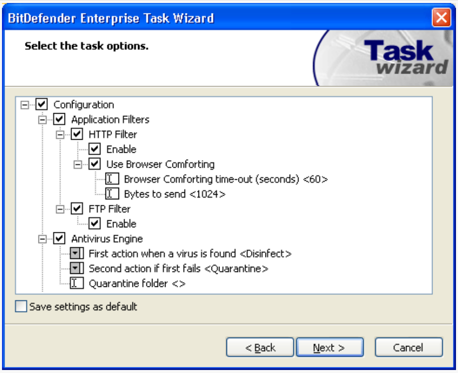
Welcome to the BitDefender Task wizard.
This wizard will help you create and schedule different tasks, and deploy them on the clients computers.

Click Next to continue.

Welcome to the BitDefender Task Wizard

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

14.1.2. Step 2/5 - Select the task options



Select the task options.

- ☑ Configuration
  - ☑ Application Filters
    - ☑ HTTP Filter
      - ☑ Enable
      - ☑ Use Browser Comforting
        - Browser Comforting time-out (seconds) <60>
        - Bytes to send <1024>
    - ☑ FTP Filter
      - ☑ Enable
  - ☑ Antivirus Engine
    - First action when a virus is found <Disinfect>
    - Second action if first fails <Quarantine>
    - Quarantine folder <>

☐ Save settings as default

Select the task options

Here you can configure BitDefender for MS ISA Servers Enterprise Edition.

The configuration options are grouped into five categories: Application Filters, Antivirus Engine, Antivirus Update, Real Time Virus Report and General.

Note

Click the box labeled "+" to open a category or click the one labeled "-" to close it.

Note

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.

Application Filters

Check the box next to the **Application Filters** category in order to set up the configuration.

The following options are available:

- **HTTP** - to set the configuration for the HTTP filter.
  - **Enable** - enables the HTTP filter;
  - **Use Browser Comforting** - select this option to avoid browser time-outs. Configure the time-out interval and the number of bytes sent during this interval.
- **FTP** - to set the configuration for the FTP filter.
  - **Enable** - enables the HTTP filter;

Antivirus Engine

Check the box next to the **Antivirus Engine** category in order to set up the configuration.

The following options are available:

- **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.
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.

Antivirus Update

Check the box next to the **Antivirus Update** category in order to set up the configuration.

The following options are available:

- **Check interval** - BitDefender allows for the selection of the update checking interval. By default this is 3 hours. If you want to change it, type in a new interval;
- **Main upgrade location** - If you are connected to a local network that has BitDefender virus signatures placed locally, you can change the location of the updates here. By default this is: http://upgrade.bitdefender.com.
- **Use proxy** - In case the company uses a proxy server check, this option. The following settings must be specified:
  - **Proxy server** - type in the IP of the proxy server;
  - **Proxy port** - type in the port the server uses to connect to the proxy server;
  - **Proxy username, if needed** - type in a user name recognized by the proxy;
  - **Proxy password, if needed** - type in the valid password for the previously specified user.

Real Time Virus Report

Check the box next to the **Real Time Virus Report** category in order to set up the configuration.

The following options are available:

- **Enable** - enables the RTVR;

- **Choose your location** - select the country you live in, from the scroll down list.

General

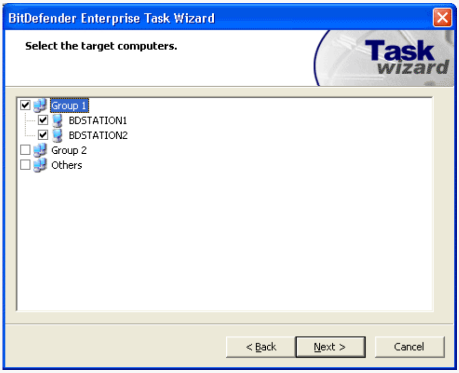
Check the box next to the **General** category in order to set up the configuration.

The following options are available:

- **Register** - to register the product;
  - **Registration key** - type in the serial number.

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

14.1.3. Step 3/5 - Select the target computers



Select the target computers

You must select the clients and/or the groups.

Note

If a group contains at least one client then a double-click on that group's name or on the icon next to it will expand that group.

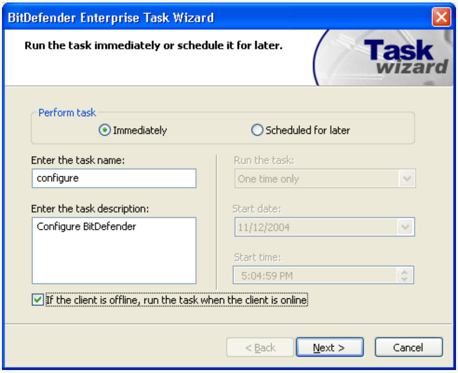
You can choose to run the task on one or several clients. To select the entire client group check the box next to that group's name.

Note

If you schedule a task on an entire client group, the task will be launched even with clients added at a later time.

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

14.1.4. Step 4/5 - Run the task immediately or schedule it for later



BitDefender Enterprise Task Wizard

Run the task immediately or schedule it for later.

Perform task: ● Immediately ○ Scheduled for later

Enter the task name: configure

Enter the task description: Configure BitDefender

Run the task: One time only

Start date: 11/12/2004

Start time: 5:04:59 PM

☑ If the client is offline, run the task when the client is online

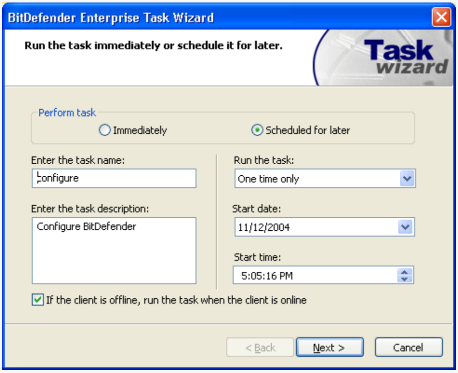
Run the task immediately

You can opt for an immediate or a programmed task.

For an immediate task, click **Immediately**. You must specify the following:

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

For a scheduled configuration, select **Scheduled for later**.



BitDefender Enterprise Task Wizard

Run the task immediately or schedule it for later.

Perform task: ○ Immediately ● Scheduled for later

Enter the task name: configure

Enter the task description: Configure BitDefender

Run the task: One time only

Start date: 11/12/2004

Start time: 5:05:16 PM

☑ If the client is offline, run the task when the client is online

Schedule the task for later

You must specify the following:

- **Enter the task name** - type in a name for the task;
- **Enter the task description** - type in a short description of the task.
- **Run the task** - it is a list of time intervals within which the task should run:
  - **One time only** - to run the task only once at a specified moment;
  - **Every hour** - to run the task every hour;
  - **Every 6 hours** - to run the task 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** - select the day from the calendar on display when the task will launch;
- **Start time** - type in the time when the task will launch.

Note

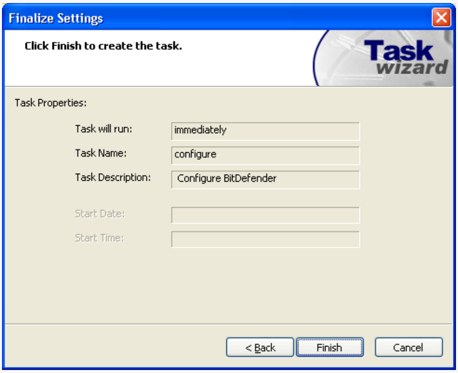
You can use the corresponding up/down arrows.

Warning

The task may fail if the target workstation is offline, therefore check the box next to **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.

14.1.5. Step 5/5 - Finalize settings



Task Properties:

Task will run: immediately

Task Name: configure

Task Description: Configure BitDefender

Start Date:

Start Time:

Finalize settings

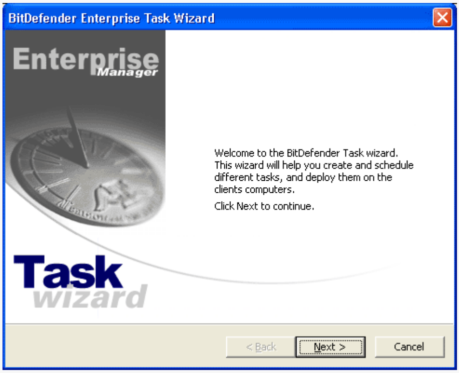
The last window of the wizard contains all the information regarding the task. You can make any changes by returning to the previous steps (**Back**). If you do not want to make any changes, click **Finish**.

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.

14.2. Get BitDefender Status

In order to obtain the BitDefender status of the selected servers, double-click the **Get BitDefender Client Status** icon (from the **Task Templates** pane). This will launch the wizard, which will guide you through the process:

14.2.1. Step 1/5 - Welcome to the BitDefender Task Wizard



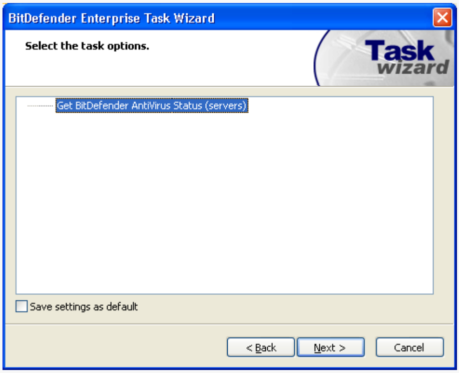
Welcome to the BitDefender Task wizard. This wizard will help you create and schedule different tasks, and deploy them on the clients computers.

Click Next to continue.

Welcome to the BitDefender Task Wizard

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

14.2.2. Step 2/5 - Select the task options



Select the task options.

Get BitDefender AntiVirus Status (servers)

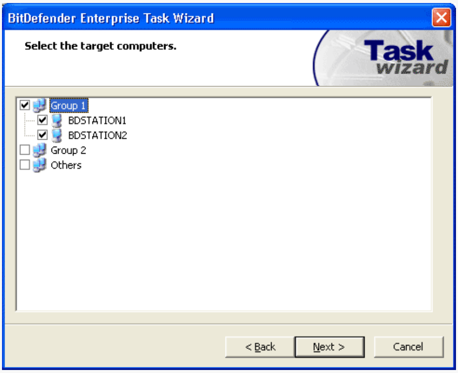
□ Save settings as default

Select the task options

Select the components you want to receive information about.

Click **Next**.

14.2.3. Step 3/5 - Select the target computers



Select the target computers

You must select the clients and/or the groups.

Note

If a group contains at least one client then a double-click on that group's name or on the icon next to it will expand that group.

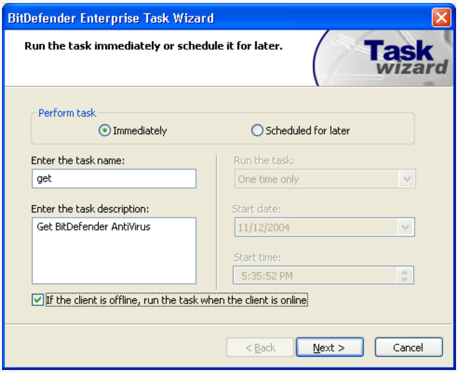
You can choose to run the task on one or several clients. To select the entire client group check the box next to that group's name.

Note

If you schedule a task on an entire client group, the task will be launched even with clients added at a later time.

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

14.2.4. Step 4/5 - Run the task immediately or schedule it for later



BitDefender Enterprise Task Wizard

Run the task immediately or schedule it for later.

Perform task: ● Immediately ○ Scheduled for later

Enter the task name: get

Enter the task description: Get BitDefender AntiVirus

Run the task: One time only

Start date: 11/12/2004

Start time: 5:35:52 PM

☑ If the client is offline, run the task when the client is online

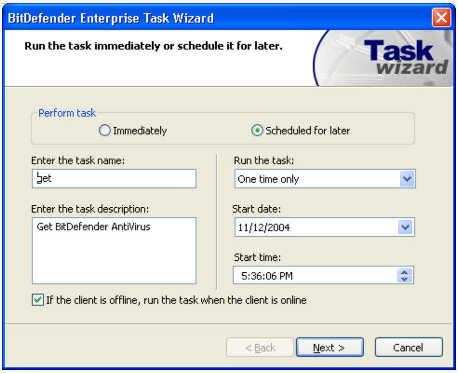
Run the task immediately

You can opt for an immediate or a programmed task.

For an immediate task, click **Immediately**. You must specify the following:

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

For a scheduled configuration, select **Scheduled for later**.



BitDefender Enterprise Task Wizard

Run the task immediately or schedule it for later.

Perform task: ○ Immediately ● Scheduled for later

Enter the task name: get

Enter the task description: Get BitDefender AntiVirus

Run the task: One time only

Start date: 11/12/2004

Start time: 5:36:06 PM

☑ If the client is offline, run the task when the client is online

Schedule the task for later

You must specify the following:

- **Enter the task name** - type in a name for the task;
- **Enter the task description** - type in a short description of the task.
- **Run the task** - it is a list of time intervals within which the task should run:
  - **One time only** - to run the task only once at a specified moment;
  - **Every hour** - to run the task every hour;
  - **Every 6 hours** - to run the task 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** - select the day from the calendar on display when the task will launch;
- **Start time** - type in the time when the task will launch.

Note

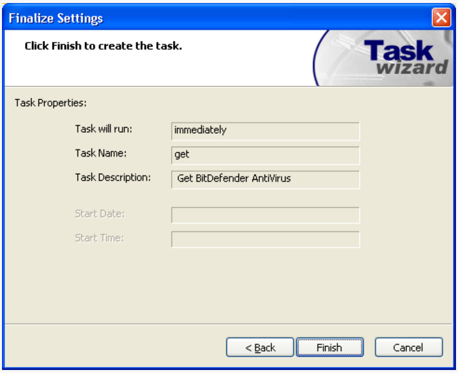
You can use the corresponding up/down arrows.

Warning

The task may fail if the target workstation is offline, therefore check the box next to **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.

14.2.5. Step 5/5 - Finalize settings



Click Finish to create the task.

Task Properties:

Task will run: immediately

Task Name: get

Task Description: Get BitDefender AntiVirus

Start Date:

Start Time:

Finalize settings

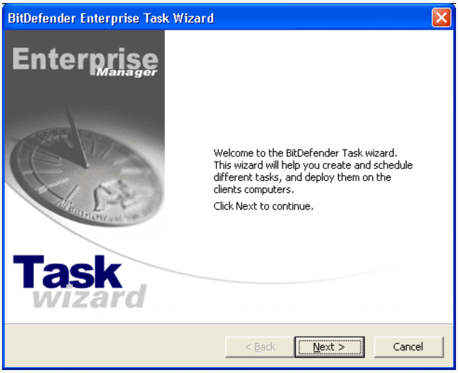
The last window of the wizard contains all the information regarding the task. You can make any changes by returning to the previous steps (**Back**). If you do not want to make any changes, click **Finish**.

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.

14.3. Get BitDefender for MS ISA Servers Enterprise Edition Statistics

In order to obtain statistics about the **BitDefender for MS ISA Servers Enterprise Edition** of the selected servers, double-click the **Get BitDefender for MS ISA Servers Enterprise Edition Statistics** icon (from the **Task Templates** pane). This will launch the wizard, which will guide you through the process:

14.3.1. Step 1/5 - Welcome to the BitDefender Task Wizard



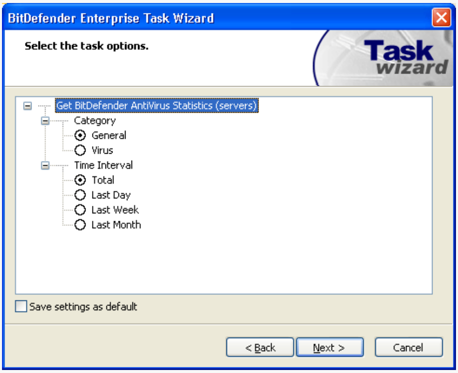
Welcome to the BitDefender Task wizard.
This wizard will help you create and schedule different tasks, and deploy them on the clients computers.

Click Next to continue.

Welcome to the BitDefender Task Wizard

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

14.3.2. Step 2/5 - Select the task options



Select the task options.

- Get BitDefender AntiVirus Statistics (servers)
  - Category
    - ● General
    - ○ Virus
  - Time Interval
    - ● Total
    - ○ Last Day
    - ○ Last Week
    - ○ Last Month

□ Save settings as default

Select the task options

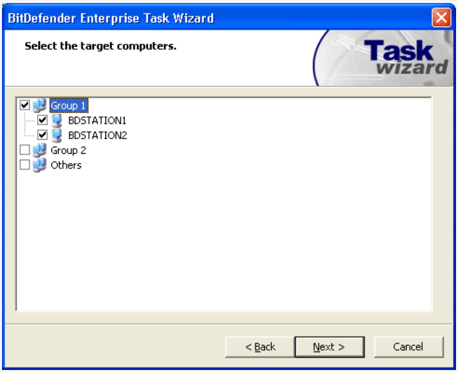
Select the category (**General** or **Virus**) and the time interval (**Total**, **Last Day**, **Last Week** or **Last Month**).

Click **Next**.

Note

In order to see the results of this task, you must create a report in the **BitDefender Enterprise Manager**. The statistics will be presented in a graphic mode.

14.3.3. Step 3/5 - Select the target computers



Select the target computers

You must select the clients and/or the groups.

Note

If a group contains at least one client then a double-click on that group's name or on the icon next to it will expand that group.

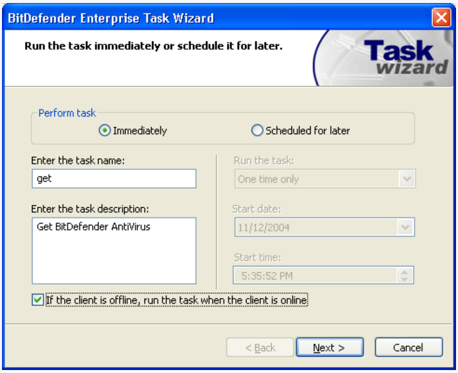
You can choose to run the task on one or several clients. To select the entire client group check the box next to that group's name.

Note

If you schedule a task on an entire client group, the task will be launched even with clients added at a later time.

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

14.3.4. Step 4/5 - Run the task immediately or schedule it for later



BitDefender Enterprise Task Wizard

Run the task immediately or schedule it for later.

Perform task: ● Immediately ○ Scheduled for later

Enter the task name: get

Enter the task description: Get BitDefender AntiVirus

Run the task: One time only

Start date: 11/12/2004

Start time: 5:35:52 PM

☑ If the client is offline, run the task when the client is online

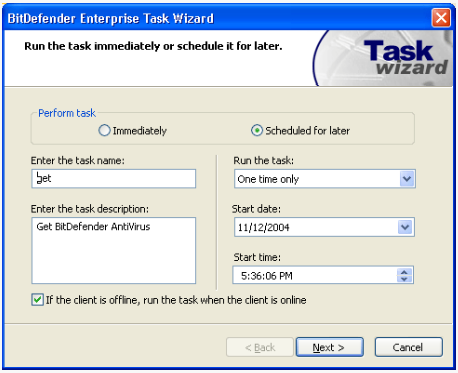
Run the task immediately

You can opt for an immediate or a programmed task.

For an immediate task, click **Immediately**. You must specify the following:

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

For a scheduled configuration, select **Scheduled for later**.



BitDefender Enterprise Task Wizard

Run the task immediately or schedule it for later.

Perform task: ○ Immediately ● Scheduled for later

Enter the task name: get

Enter the task description: Get BitDefender AntiVirus

Run the task: One time only

Start date: 11/12/2004

Start time: 5:36:06 PM

☑ If the client is offline, run the task when the client is online

Schedule the task for later

You must specify the following:

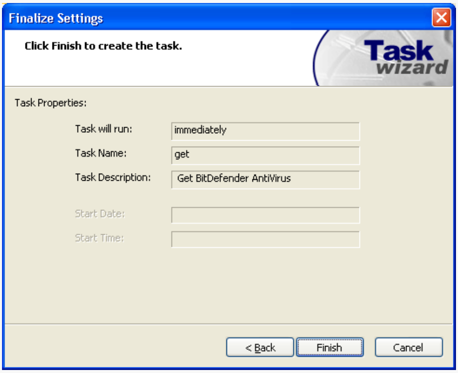
- **Enter the task name** - type in a name for the task;
- **Enter the task description** - type in a short description of the task.
- **Run the task** - it is a list of time intervals within which the task should run:
  - **One time only** - to run the task only once at a specified moment;
  - **Every hour** - to run the task every hour;
  - **Every 6 hours** - to run the task 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** - select the day when the task will launch from the calendar on display;
- **Start time** - type in the time when the task will launch.

> **Note**
> You can use the corresponding up/down arrows.

> **Warning**
> The task may fail if the target workstation is offline, therefore check the box next to **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.

14.3.5. Step 5/5 - Finalize settings



Click Finish to create the task.

Task Properties:

Task will run: immediately

Task Name: get

Task Description: Get BitDefender AntiVirus

Start Date:

Start Time:

Finalize settings

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

15. Frequently Asked Questions

Q: What are the system requirements?

A: You will find them in the “*System Requirements*” (p. 9) section.

Q: How can I register BitDefender?

A: The registration procedure is described in the “*Product Registration*” (p. 71) section.

Q: How can I tell if BitDefender is actually working?

A: Use the EICAR test described in the Best practices section.

Q: BitDefender is not working. What should I do?

A: Check whether the BitDefenders filters are enabled on the Microsoft ISA user interface and on the BitDefender Management Console.

Q: How can I disable BitDefender?

A: Access the Application Filters and disable the HTTP & FTP filters.

Q: Is it possible to scan only audio files?

A: Yes it is. You must create a specific filtering rule.

Q: How can I update BitDefender?

A: By default, BitDefender will automatically update every 3 hours. But you can also update manually or change the time interval for the automatic update in the Antivirus Update section.

Q: How can I perform a manual update?

A: Access the Antivirus Update section, click **Configure BitDefender Update** and click **Update now!**.

Q: Why is it necessary to update the BitDefender scanning engines?

A: Every time you perform an update new virus&spyware definitions will be added to the scan engines.

Q: How do I uninstall BitDefender?

A: The removing procedure is described in the “*Uninstalling or Repairing BitDefender*” (p. 12) section.

16. Support

16.1. 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.

16.2. On-line Help

16.2.1. 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.

16.3. 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.

16.3.1. 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

16.3.2. 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:
Email: <support@bitdefender.com>
Customer Service: 954-776-6262
http://www.bitdefender.com

Romania

SOFTWIN
5th Fabrica de Glucoza St.
PO BOX 52-93
Bucharest
Technical support: <support@bitdefender.ro>
Sales: <sales@bitdefender.ro>
Phone: +40 21 2330780
Fax: +40 21 2330763
Product web site: http://www.bitdefender.ro