# BitDefender for MS ISA Server 2004 Enterprise Edition

Quickstart

bitdefender
secure your every bit

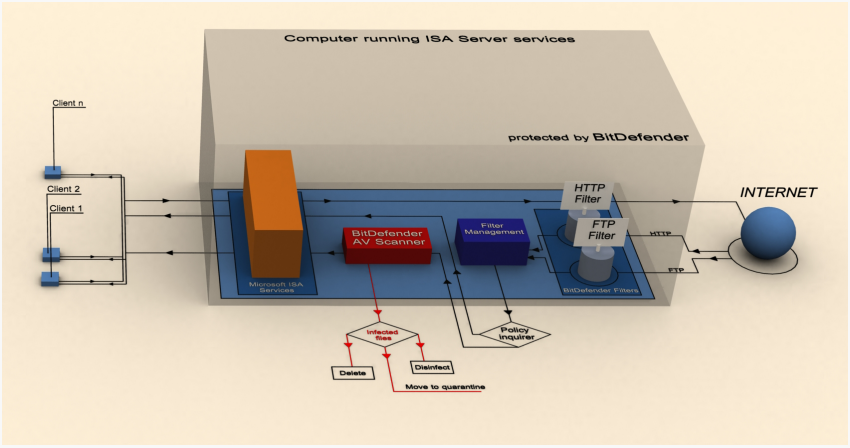
# 1. How Does It Work?

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 Server 2004 Enterprise Edition** offers antivirus and antispyware protection for web traffic, including files received via web mail. **BitDefender for MS ISA Server 2004 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 Server 2004 Enterprise Edition** is compatible with **BitDefender for Mail Servers (WIN SMTP Proxy)** which offers antivirus and antispam protection for SMTP traffic.

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



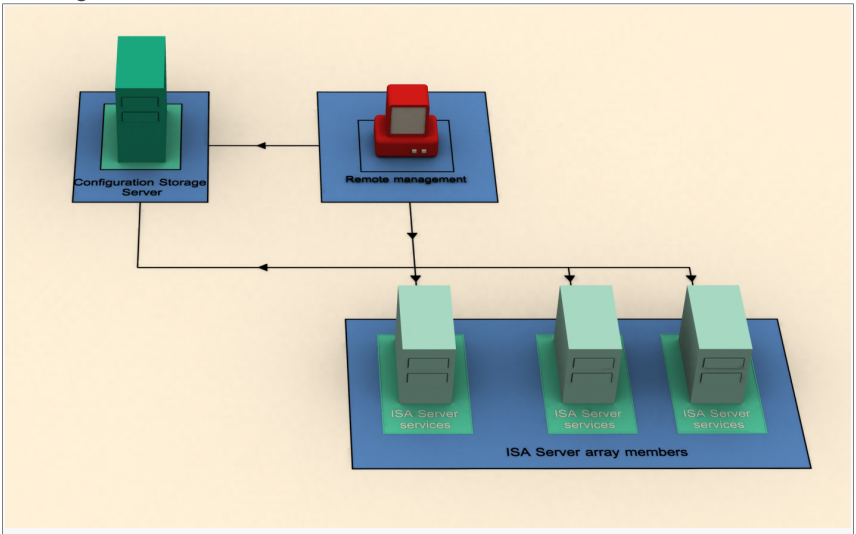

Working schema

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 (**Policies -> Rules**).

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 Microsoft ISA Server 2004 Enterprise Edition, see the design below:




Working schema

**BitDefender for MS ISA Server 2004 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 Server 2004 Enterprise Edition** can be administered either remotely, from the management console of , or directly, from the respective computer. The advantage of using  is that all BitDefender products can be configured and monitored from only one terminal, which saves time and money.

# 2. Main Features

**BitDefender for MS ISA Server 2004 Enterprise Edition** offers antivirus and antispyware protection for web traffic, including files received via web mail.

| Feature | Benefits |
|---|---|
| **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 Server 2004 En- |

| Feature | Benefits |
|---|---|
| | terprise 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 Server 2004 Enterprise Edition makes use of a comprehensive database of spyware signatures to filter traffic and protect clients against such threats. |
| **Integrated with Microsoft ISA Server 2004 Enterprise Edition** | BitDefender for MS ISA Server 2004 Enterprise Edition seamlessly integrates with Microsoft ISA Server 2004 Enterprise Edition through two application filters, an HTTP and an FTP filter. |
| **Protection for Server Arrays** | BitDefender for MS ISA Server 2004 Enterprise Edition protects all the arrays of the enterprise that run Microsoft ISA Server 2004 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 Server 2004 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 |

| Feature | Benefits |
|---|---|
| | 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 Server 2004 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 Server 2004 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 Server 2004 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 Server 2004 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 Server 2004 Enterprise Edition is fully compatible with , offering organizations centralized management for antivirus and anti- |

| Feature | Benefits |
|---|---|
| | spyware 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. |

# 3. System Requirements

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

# 4. 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. Access the **Alerts** section (**Configuration -> Alerts**) and click **Configure BitDefender Alerts** to configure the alerts.

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**).

# 5. Contact information

As a valued provider, SOFTWIN strives to offer its costumers an unparalleled level of fast and accurate support. The Support Center (which you can contact at the address indicated below) continually keeps up with the latest threats. This is where all your questions are answered in due time.

With SOFTWIN, 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 costumer support. During the past ten years, SOFTWIN has gained 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.

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