

# BitDefender for MS SharePoint 2003

## User Guide

# Table of Contents

<b>Terms of agreement</b> .....	<b>4</b>
<b>Software licensing</b> .....	<b>4</b>
<b>License and warranty</b> .....	<b>5</b>
<b>Installation</b> .....	<b>8</b>
<b>System requirements</b> .....	<b>8</b>
<b>Installation steps</b> .....	<b>8</b>
<b>Uninstalling or repairing BitDefender</b> .....	<b>9</b>
<b>Introduction</b> .....	<b>10</b>
<b>How does it work?</b> .....	<b>10</b>
<b>BitDefender Main Features</b> .....	<b>11</b>
<b>The User Interface</b> .....	<b>12</b>
<b>Access</b> .....	<b>12</b>
<b>General view</b> .....	<b>12</b>
<b>Product Registration</b> .....	<b>14</b>
<b>Scan options</b> .....	<b>15</b>
Selecting the action on infected files .....	<b>15</b>
Specifying the quarantine zone .....	<b>16</b>
<b>On-access scanner</b> .....	<b>17</b>
<b>On-demand scanner</b> .....	<b>19</b>
<b>Antivirus update</b> .....	<b>22</b>
Configuring the update .....	<b>22</b>
Viewing update information .....	<b>23</b>
<b>Mail notification</b> .....	<b>24</b>

<b>Reports .....</b>	<b>26</b>
Creating a scan report .....	26
Viewing a scan report .....	27
<b>Real Time Virus Report .....</b>	<b>28</b>
<b>Best practices .....</b>	<b>29</b>
<b>Frequently Asked Questions .....</b>	<b>31</b>
<b>BitDefender Enterprise Manager Integration .....</b>	<b>32</b>
<b>Description and features.....</b>	<b>32</b>
<b>Supported clients .....</b>	<b>34</b>
<b>How does it work? .....</b>	<b>34</b>
Working schema .....	35
BitDefender Server .....	36
BitDefender Local Manager .....	37
BitDefender Management Console .....	37
BitDefender Deployment Tool .....	38
BitDefender Update Server .....	38
<b>Additional Task Templates .....</b>	<b>39</b>
Configuring BitDefender for MS SharePoint 2003 .....	41
BitDefender Antivirus .....	42
Reports and Notifications .....	43
BitDefender Information.....	44
Retrieving BitDefender statistics.....	46
Retrieving BitDefender status.....	48
Retrieving a list with all BitDefender products installed .....	50
Sending a message to clients.....	52
Configuring Windows Update .....	54
Retrieving Windows Update status.....	57
<b>Contact information .....</b>	<b>60</b>

# Terms of agreement

## Software licensing

The BitDefender package is protected by the copyright law and the international treaties regarding the copyright, as well as other laws and treaties regarding the intellectual property.

The copyright law, as well as other intellectual property laws, protects in many countries the software owner's rights, according them some exclusive rights including the right to reproduce and copy the software. Copying the software without the owner's permission represents "copyright infringement" and the law imposes penalties and punishments.

Software is considered to be copied when:

- Loading the software in your computer's memory through running it from the floppy disk, hard disk, CD-ROM, or other media;
- Copying the software to another medium, such as floppy disk or hard disk;
- Running the program on the computer from a network server where the software is resident or deposited.

Almost any commercial software is directly or indirectly licensed by the copyright owner (the software developer) for final usage through a so-called licensing contract. The software products may have different types of licensing contracts.

BitDefender is a trademark of SOFTWIN. Microsoft, Windows, Excel, Word, and the Windows logo, Windows NT, and Windows 2000 are registered trademarks of Microsoft Corporation. All other trademarks are the property of their respective owners.

## License and warranty

IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS DO NOT INSTALL THE SOFTWARE. BY CLICKING "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.

This License Agreement is a legal agreement between you and SOFTWIN for use of the SOFTWIN software product identified above, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("BitDefender"), all of which are protected by U. S. and international copyright laws and international treaty protection. By installing, copying, or otherwise 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; you may, however, return it to your place of purchase for a full refund within 30 days after your purchase. Verification of your purchase may be required.

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 license to use BitDefender:

**APPLICATION SOFTWARE.** You may install and use one copy of BitDefender, or any prior version for the same operating system, on a single computer terminal. The primary user of the computer on which BitDefender is installed may make one additional (i.e. second) copy for his or her exclusive use on a portable computer.

**NETWORK USE.** You may also store or install a copy of BitDefender on a storage device, such as a network server, used only to install or run BitDefender on your other computers over an internal network; however, you must purchase and dedicate a separate license for each separate computer terminal on which BitDefender is installed or run from the storage device. A license for BitDefender may not be shared or used concurrently on different computers or computer terminals. You should purchase a license pack if you require multiple licenses for use on multiple computers or computer terminals.

**LICENSE PACKS.** If you purchase a License Pack and you have acquired this License Agreement for multiple licenses of BitDefender, you may make the number of additional copies of the computer software portion of BitDefender specified above as "Licensed copies." You are also entitled to make a corresponding number of secondary copies for portable computer use as specified above in the section entitled "Application Software".

**LICENSE TERMS.** The license granted hereunder shall commence on the date that you install, copy or otherwise first use BitDefender and shall continue only on the computer on which it is initially installed.

**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 have 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 on more than one computer.

**COPYRIGHT.** All rights, title 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 except that you may install BitDefender on a single computer provided you keep the original solely for backup or archival purposes. 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, or lease BitDefender. 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.

SOFTWIN HEREBY DISCLAIMS ALL OTHER WARRANTIES FOR BITDEFENDER, WHETHER EXPRESSED OR IMPLIED. THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESSED OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

**DAMAGES DISCLAIMER.** 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 or 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.

GOVERNMENT RESTRICTED RIGHTS/RESTRICTED RIGHTS LEGEND. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of Commercial Computer Software-Restricted Rights clause at 48 CFR 52.227-19, as applicable. Contact SOFTWIN, at Fabrica de Glucoza St., No 5, 72322-Sect.2, Bucharest, Romania, or at Tel No: 40-21-2330780 or Fax: 40-21-2330763.

GENERAL. This Agreement will be governed by the Romanian laws and by the international copyright regulations and treaties. This Agreement may only be modified by a license addendum, which accompanies this Agreement or by a written document, which has been signed, by both you and SOFTWIN. This Agreement has been written in the English language only and is not to be translated or interpreted in any other language. 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. Microsoft, Windows, Excel, Word, the Windows logo, Windows NT, Windows 2000 are registered trademarks of Microsoft Corporation. All other trademarks are the property of their respective owners.

# Installation

## System requirements

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

- ➔ Microsoft SharePoint Portal Server 2003 or
- ➔ Microsoft Windows SharePoint Services v 2.0

## Installation steps

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



Figure 1

Installation steps:

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

 **Note**

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

## Uninstalling or repairing BitDefender

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

A new window will appear where you can select:

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

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

# Introduction

## How does it work?

**BitDefender for MS SharePoint 2003** performs real-time scanning of uploaded and downloaded files in the document libraries and lists, with excellent cleanup rates, and an option to quarantine infected documents. The on-demand scanner and advanced reporting and logging tools further enhance the value of **BitDefender for MS SharePoint**, as a security solution for your collaboration needs.

The schema below shows the way BitDefender works:

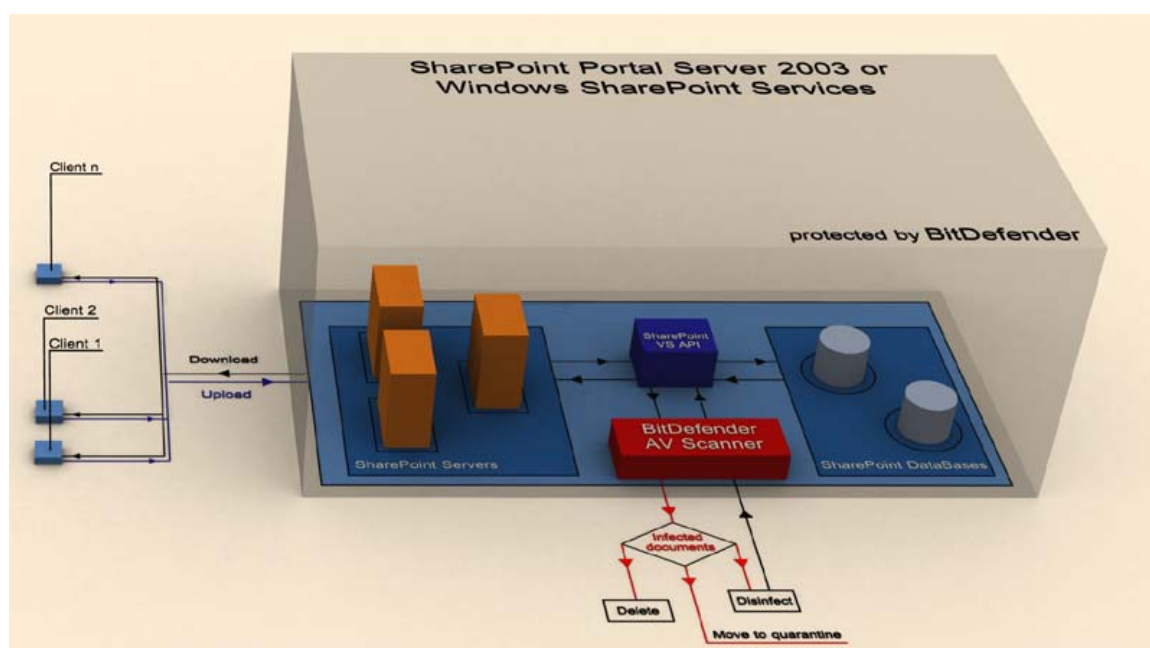


Figure 2

Whenever a document is uploaded or downloaded, it is immediately scanned through VS API. If BitDefender Antivirus Scanner finds an infection, the document will be treated conforming to the options selected by the administrator. Alarm messages will eventually be sent through e-mail to the competent persons.

As you can see, only the clean documents can be downloaded&uploaded from the Microsoft SharePoint on the workstations and opposite. Getting infected with the documents stored on the Microsoft SharePoint Server becomes practically impossible.

The infected documents are treated depending on the administrator's option, by disinfection, deletion or isolation on a certain location (the quarantine zone).

# BitDefender Main Features

**BitDefender for MS SharePoint 2003** seamlessly integrates with Microsoft SharePoint® Portal Server 2003 and with Microsoft Windows SharePoint Services. While Microsoft SharePoint® Portal Server 2003 provides facilities for team collaboration and makes it easier for users to work together on documents by sharing information, **BitDefender for MS SharePoint 2003** provides antivirus protection for your SharePoint Server.

## KEY FEATURES

## BENEFITS

### Certified Antivirus Engines

**BitDefender for MS SharePoint 2003** ensures antivirus protection by incorporating the BitDefender antivirus engines, certified by ICSA Labs, Checkmark, CheckVir, Virus Bulletin and TUV.

### Improved Virus Detection

**BitDefender for MS SharePoint 2003** ensures antivirus protection by incorporating the BitDefender antivirus engines, certified by ICSA Labs, Checkmark, CheckVir, Virus Bulletin and TUV.

### Scan the Upload/Download Files from and to Document Libraries and Lists

**BitDefender for MS SharePoint 2003** scans for viruses all the files which are uploaded or downloaded through Microsoft SharePoint® Portal Server 2003 in document libraries or lists, ensuring real-time antivirus protection and prevents the spreading of viruses in your organization.

### Automatic Updating

**BitDefender for MS SharePoint 2003** offers intelligent updates with new virus definitions and restricted content database. Due to seamless integration with the Microsoft SharePoint® Portal Server 2003, the antivirus protection is not discontinued while updating the virus signatures. Upon a new request for a specific document, **BitDefender for MS SharePoint 2003** rescans it with the new signatures.

### On-Demand Scanning of Files

**BitDefender for MS SharePoint 2003** includes an on-demand scanning module, which provides the possibility to scan whole document libraries or lists.

### Reports and Notifications

**BitDefender for MS SharePoint 2003** comes with a useful “Reports and Logs” module that provides detailed information about the scanned files. The “Notification” module is a tool used to alert the administrator in case a virus, warning or error occurred.

### Centralized Management from a Network Location

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

### 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 pricing offers are available to returning clients.

### 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.

# The User Interface

## Access

To access the **BitDefender for MS SharePoint 2003** interface you must follow the next steps:

1. Access the default **Microsoft SharePoint 2003 Server** page;
2. Click **Site Settings** (upper right corner);
3. Click **Go to SharePoint Portal Server central administration** from the **General Settings** section;
4. Click **BitDefender for MS SharePoint Settings** in the left pane;

or quicker access the **Sharepoint Central Administration** and click **BitDefender for MS SharePoint Settings** from the left pane.



Administrator password for **Microsoft SharePoint Server 2003** is required to access the interface.

## General view

The access to the user interface is made through the Windows Start menu, by following the path **Start → Programs → BitDefender for File Servers → BitDefender for File Servers**.

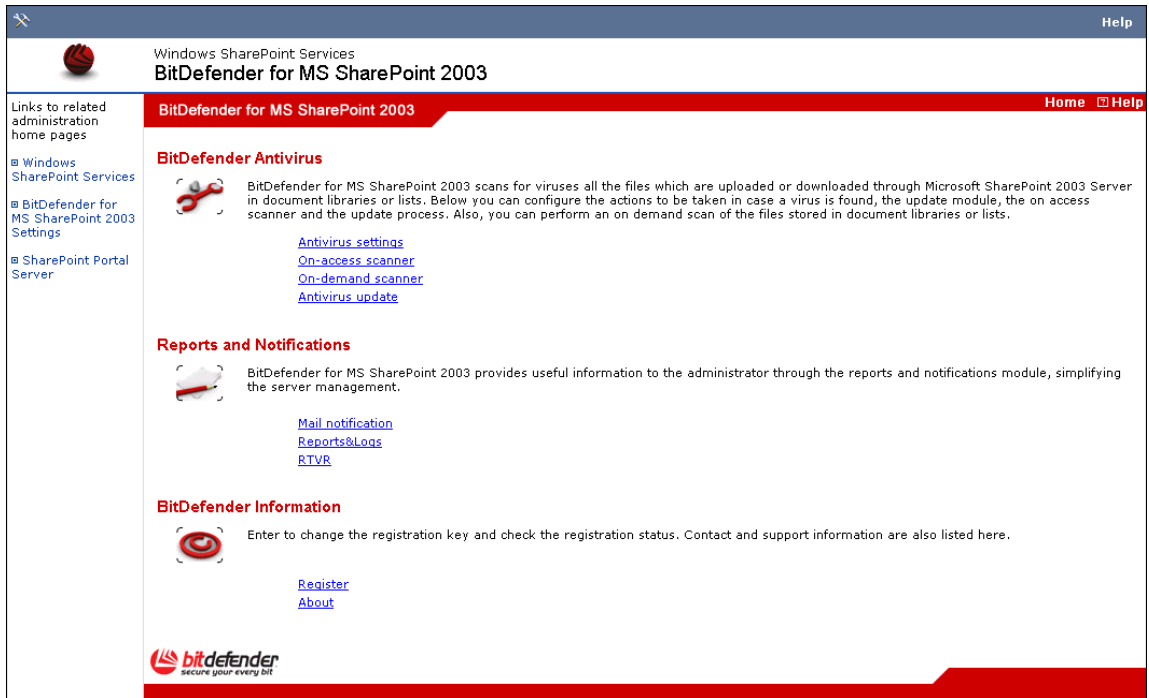


Figure 3

The configuration window is divided in three sections: **BitDefender Antivirus**, **Reports and Notifications** and **BitDefender Information**.

### BitDefender Antivirus

The following options are available:

- [Antivirus settings](#) – to specify the scan options for the on-access scanning process;
- [On-access scanner](#) - to select the action, in case an infected file is detected, and the location of the quarantine area;
- [On-demand scanner](#) – to select the workstations where net send alerts will be send;
- [Antivirus update](#) – to select the e-mail addresses where alarm messages will be send in case of virus detection.

### Reports and Notifications

The following options are available:

- [Mail notification](#) - to access the configuration window for the product update;
- [Reports&Logs](#) – to access the virus reporting section;
- [RTVR](#) – to create and view the statistics about the scanned objects.

### BitDefender Information

The following options are available:

- [Register](#) – to access the section where you can register BitDefender;
- [About](#) – to access the section where you can see the contact information and the product details.

If you want to open the help file you must click **Help** – upper right corner.

# Product Registration

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

To modify the default serial number, click **Register** from the user interface (**BitDefender Information** section).

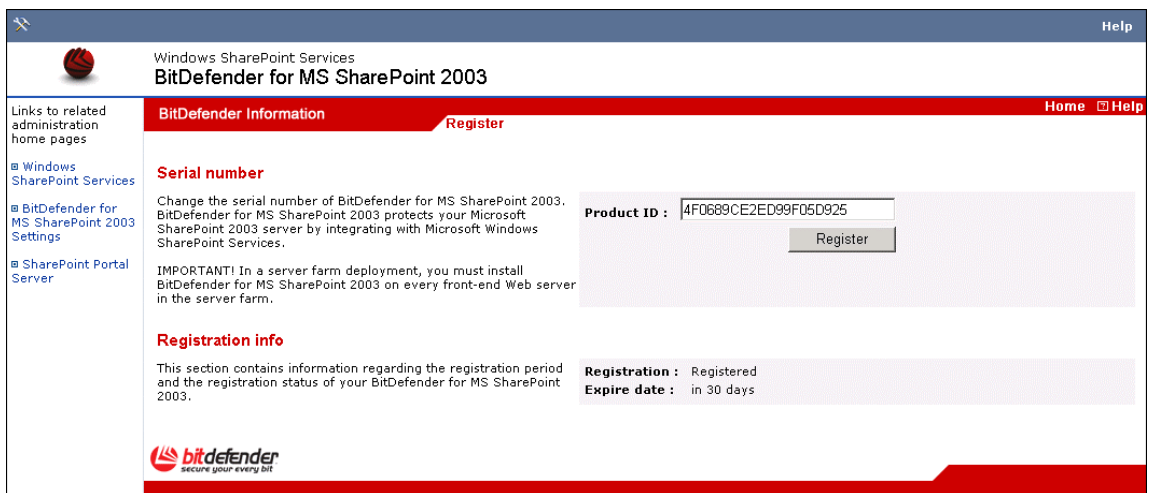


Figure 4

The window offers information about the status of the product (registered or not) and the expiration date. To register your product you must first type in the license key in the **Product ID** field. Click **Register** to finish the registration process.

In the **Register** section now, you can see the expiring date of the new license key.

# Scan options

To specify the scan options, click **Antivirus settings** from the user interface (BitDefender antivirus section).

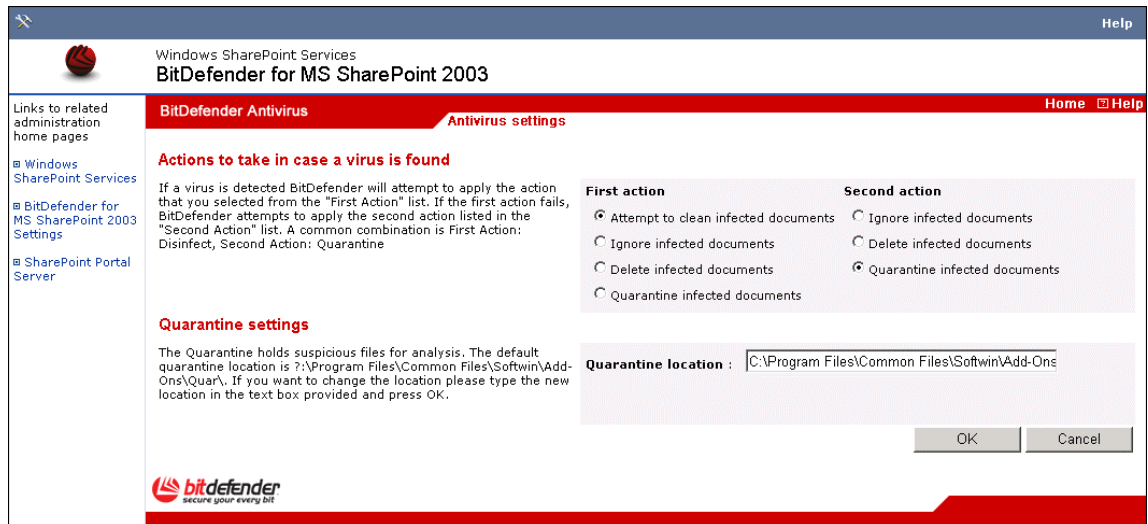


Figure 5

## Selecting the action on infected files

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

First action	Description
Attempt to clean infected documents	To disinfect the infected documents.
Ignore infected documents	To ignore the infected documents. No action will be taken on them.
Delete infected documents	To delete the infected documents.
Quarantine infected documents	To isolate the infected documents in the quarantine zone.

The **Second action** is a supplementary measure of protection and it is activated only if the first action is **Attempt to clean infected documents**.

Second action	Description
Ignore infected documents	To ignore the infected documents. No action will be taken on them.
Delete infected documents	To delete the infected documents.
Quarantine infected documents	To isolate the infected documents in the quarantine zone.

After selecting the first & the second action click **OK** to save the changes.

## Specifying the quarantine zone

The default location of the quarantine zone is:

`C:\Program Files\Common Files\Softwin\ADD-ONS\quar.`

If you want to change it, type in the complete path in the **Quarantine location** field.

Click **OK** to save the changes.

## On-access scanner

To enable the antivirus protection on your SharePoint Server, you have to configure the antivirus settings of your SharePoint Server.

Click **On-access scanner** from the user interface (**BitDefender antivirus** section).

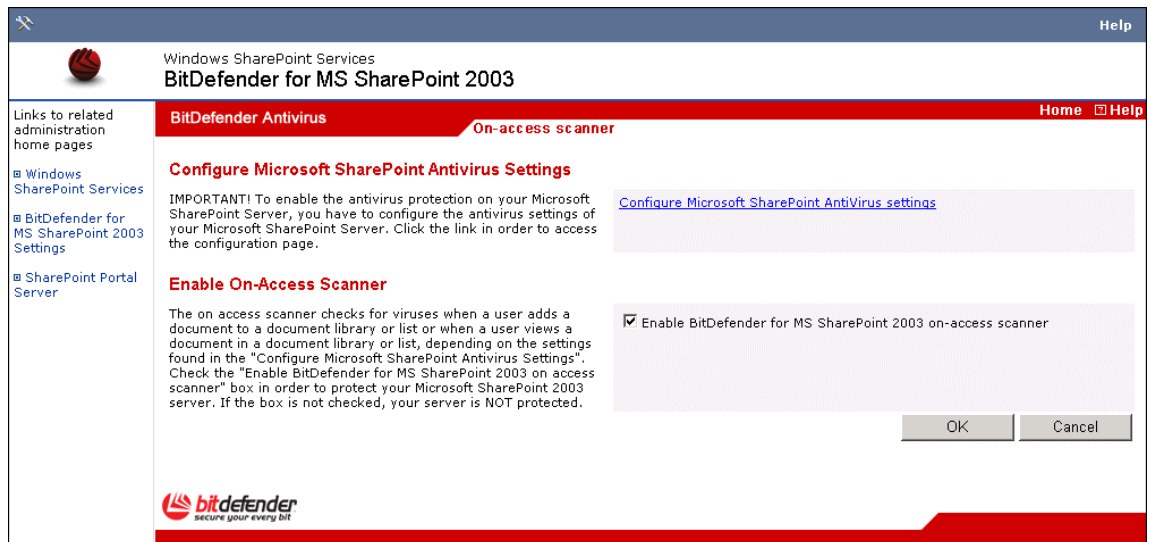
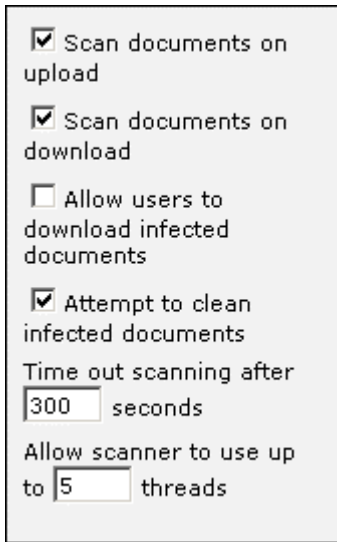


Figure 6

Click **Configure MS SharePoint Antivirus Settings** in order to access the configuration page.

The next options are available:

- **Scan documents on upload** - files are checked for viruses when a user adds a document to a document library or list.
- **Scan documents on download** - files are checked for viruses when a user views a document in a document library or list.
- **Allow user to download infected documents** - allow users to save infected files locally.
- **Attempt to clean infected documents** - if a virus is found, the scanner attempts to clean the file. You can select the actions BitDefender will take on infected documents in the [Antivirus settings](#) module.
- **Time out scanning after  $xyz$  seconds** - type the number of seconds to allow before timing out the scanning process. The default time is 300 seconds.
- **Allow scanner to use up to  $x$  threads** - type the number of threads to allow the scanning process to take up. By default, the number of threads is 5.



The screenshot shows a settings window for the BitDefender on-access scanner. It contains the following options:

- Scan documents on upload
- Scan documents on download
- Allow users to download infected documents
- Attempt to clean infected documents
- Time out scanning after  seconds
- Allow scanner to use up to  threads

**Figure 7**

Select the check boxes corresponding to:

- Scan documents on upload
- Scan documents on download
- Attempt to clean infected documents

After selecting them you have to return to the **On-access scanner** section from BitDefender and select the check box corresponding to **Enable BitDefender for MS SharePoint 2003 on-access scanner**.

Click **OK** to save the changes.

From now on, every time a document is uploaded or downloaded through MS SharePoint 2003 Server, it is immediately scanned. If an infection is found, the document will be treated conforming to the options selected by the administrator in the [Antivirus settings](#) module.

# On-demand scanner

The main objective for BitDefender is to keep all your databases clean of viruses. This is first and foremost done by keeping new viruses out of your MS SharePoint (through [On-access scanner](#) module), but there is a risk that a virus is already lodged in your databases, before you even install BitDefender.

This is why it's a very good idea to scan all your databases for resident viruses after you've installed BitDefender. And it's definitely a good idea to frequently scan all your databases for viruses.

To scan your document libraries for viruses, please follow the next steps:

## 1. Make sure that BitDefender knows the latest viruses

Before you let BitDefender scan your databases you should make sure that BitDefender is up to date with its virus signatures, since new viruses are found and identified every day. You can verify when the last update was made in the lower side of the [Antivirus update](#) module - **Last update** date.

If this date is not recent, you should let BitDefender update its virus signatures. This is very easy, and all you have to do is to click the **Update now** button - same section.

## 2. Choose scan targets

Enter the [On-demand scanner](#) module from BitDefender (click **On-demand scanner** from the user interface - **BitDefender antivirus** section).

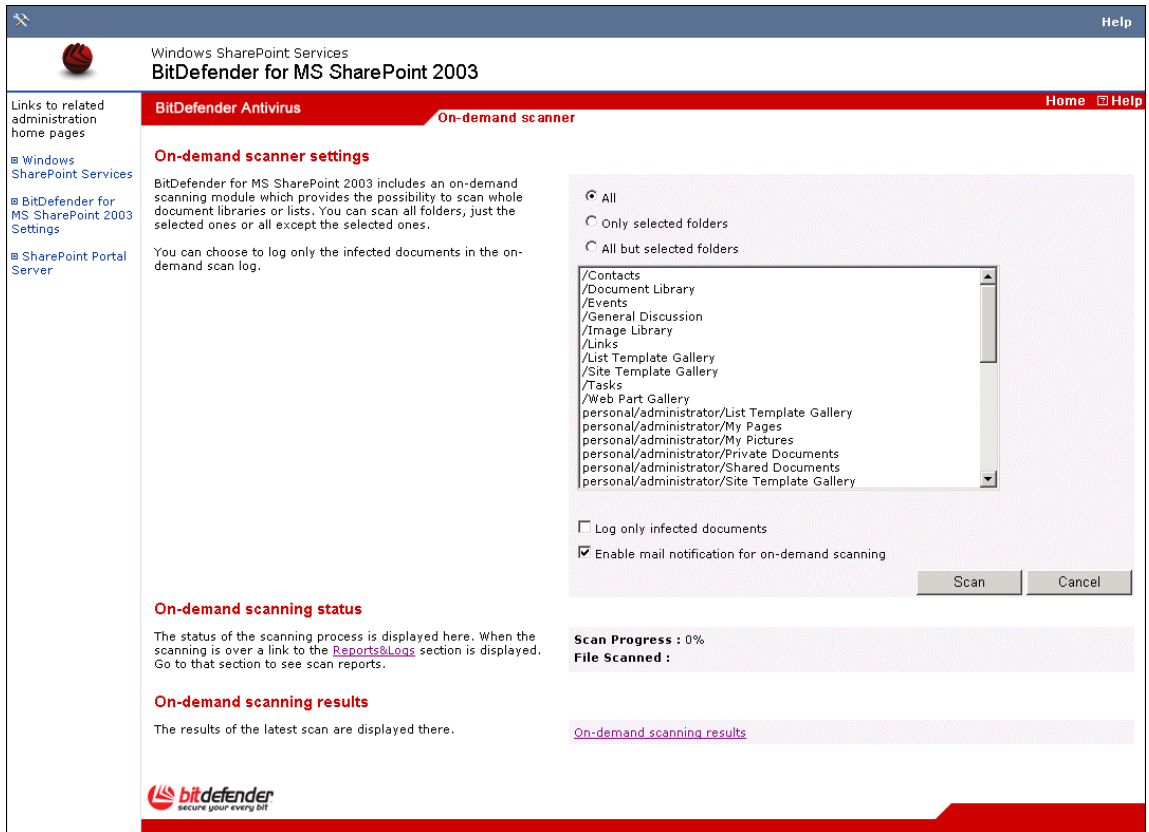


Figure 8

By default, the section contains a list with all the document libraries. Besides this, some buttons and options can also be observed.

You have three options:

- To scan all libraries - Check **All**.
- To scan only the selected libraries - Check **Only selected folders** and select the document libraries.
- To scan all libraries except the selected ones - Check **All but selected folders** and select the document libraries to be excepted from scanning

**TIP:** Use CTRL to select as many libraries as you want.

### 3. Select the report options

A report file is automatically created and it contains the name of the scanned documents, their status (clean or infected), the virus names for the infected documents and the action BitDefender took on infected documents.

In this report you can see all the scanned files or only the infected ones (if you checked **Log only infected documents** in the [On-demand scanner](#) module).

### 4. Scan for viruses

After selecting the scan target, all you have to do is to effectively start the scanning process. For that, just click **Scan**. This may take a while, depending on the size of your document libraries.

While scanning, BitDefender will show you the scan progress and the name of the current scanned file.

If the [Mail Notifications](#) module is configured, select the check box corresponding to **Enable mail notification for on-demand scanning** to be notified when viruses are found.

**TIP:** Click **Cancel** to stop the scanning process anytime you want.

### 5. Open the report file

To open the report file you have to access the [Reports](#) module, select the file and click **View last on-demand scanning log**.

The path to the report file is:

```
Program Files\Common Files\Softwin\Statistics\OnDemandReport.html
```

# Antivirus update

New viruses are found and identified every day. This is why it is very important to keep BitDefender up to date with the latest virus signatures. By default, BitDefender automatically checks for updates every eight hours.

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

Click **Antivirus update** from the user interface (**BitDefender antivirus** section).

The screenshot shows the BitDefender Antivirus update settings for MS SharePoint 2003. The interface is titled "BitDefender Antivirus" and "Antivirus update". It features a navigation menu on the left with links to "Windows SharePoint Services", "BitDefender for MS SharePoint 2003 Settings", and "SharePoint Portal Server". The main content area is divided into two sections: "Update Settings" and "Update Information".

**Update Settings:** This section contains instructions on how to update BitDefender. It includes a "Check interval" dropdown menu set to "8" hours, an "Update location" text box containing "http://upgrade.bitdefender.com", and a "Use Proxy" checkbox. Below the checkbox are four text boxes for "Server", "Port", "User", and "Password". An "Update now" button is located at the bottom of this section.

**Update Information:** This section displays the current status of the update process. It shows "Progress" at 0%, "Status" as "OK", and "Last Update" as "Thu Mar 17 12:49:06 2005".

The BitDefender logo is visible at the bottom left of the interface.

Figure 9

The module is divided in two sections: **Update settings** and **Update information**.

## Configuring the update

In the **Update settings** section you can change the automatic update interval, the update location and you can introduce the proxy settings (in case the company uses a proxy server).

- ➔ By default BitDefender checks for updates every 8 hours. If you want to modify the update interval, type a new one in the **Check interval** field.
- ➔ 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>.

- In case you are using a proxy server with authentication, select the **Use proxy** check box. You must introduce the following information
- **Server** - type in the IP of the proxy server.
  - **Port** - type in the port the server uses to connect to the proxy server.
  - **User** - type in a user name recognized by the proxy.
  - **Password** - type in the valid password for the previously specified user.

 **Note**

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

Click **OK** to save the changes.

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

## Viewing update information

In the **Update information** section you can see details regarding the product update.

**Last Checked** represents the last time BitDefender for MS SharePoint checked the BitDefender Update Server for new virus definitions.

The **Last Update** information represents the last time BitDefender for MS SharePoint 2003 downloaded new virus definitions.

You can also see the status and the progress of the update process.

# Mail notification

If an unexpected situation appears or a virus is found, there is the possibility of sending alarm messages by e-mail.

To configure this feature you must access the **Mail notification** module from the user interface (click **Mail notification** from the **Reports & Notifications** section).

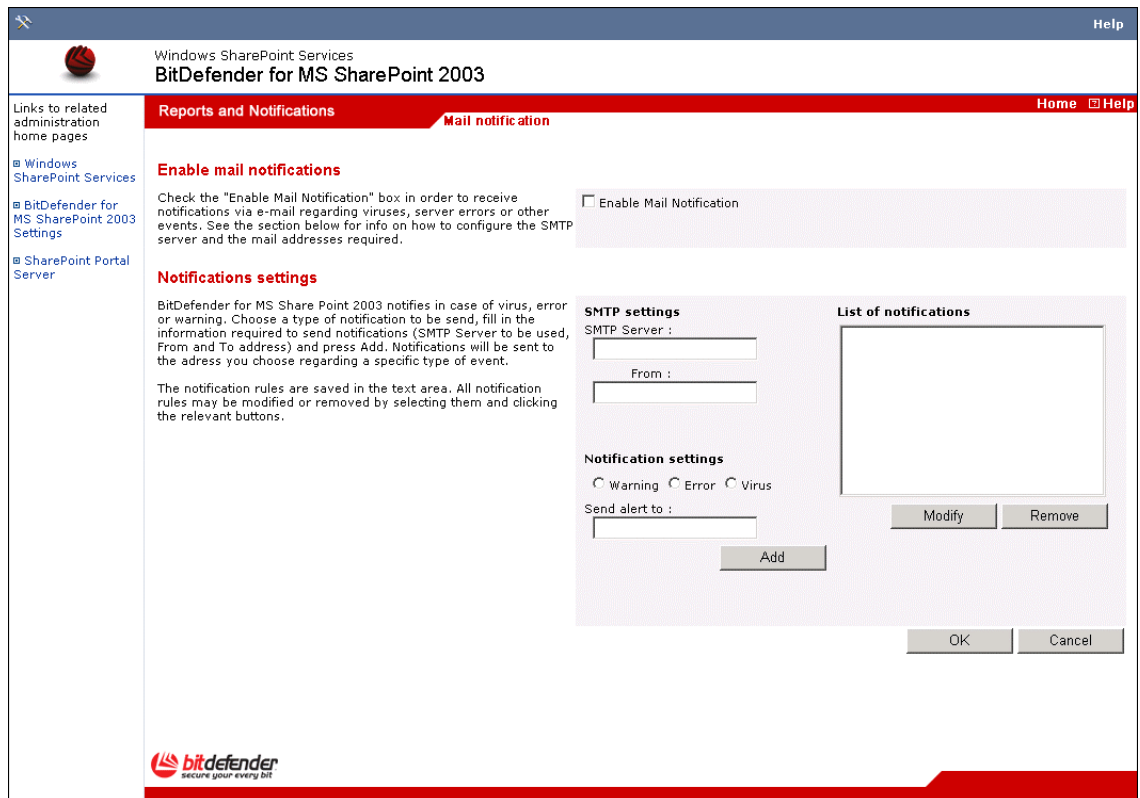


Figure 10

Types of events that can generate alarm messages.

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

To activate the **Mail Notification** service, you must select the check box corresponding to **Enable Mail Notification**.

In order to receive alerts via e-mail you must follow the next steps:

### 1. Introduce the SMTP server

Type in the SMTP server in the corresponding field (**SMTP settings** section).

### 2. Introduce the e-mail address that will appear in the sender field

Type in the e-mail address in the **From** field (**SMTP settings** section).

 **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.

### 3. Select the event when you will be notified

Select the type of event (**Warning**, **Error** or **Virus**) in the **Notification settings** section.

### 4. Introduce the e-mail address that will receive the mail notification

Type in the e-mail address in the **Send alert to** field (**Notification settings** section).

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

### 5. Introduce the e-mail address in the list of notifications

Click **Add**. The address will be added in the list of notifications.

 **Note**

If you want to change a list entry (the e-mail recipient or the event type), select it and click **Modify**. If you want to remove a list entry, select it and click **Remove**.

Finally, click **Ok** to save the changes.

# Reports

If you want to create and view report files regarding the antivirus activity you must access the **Reports&Logs** module from the user interface (click **Reports&Logs** from the **Reports & Notifications** section).

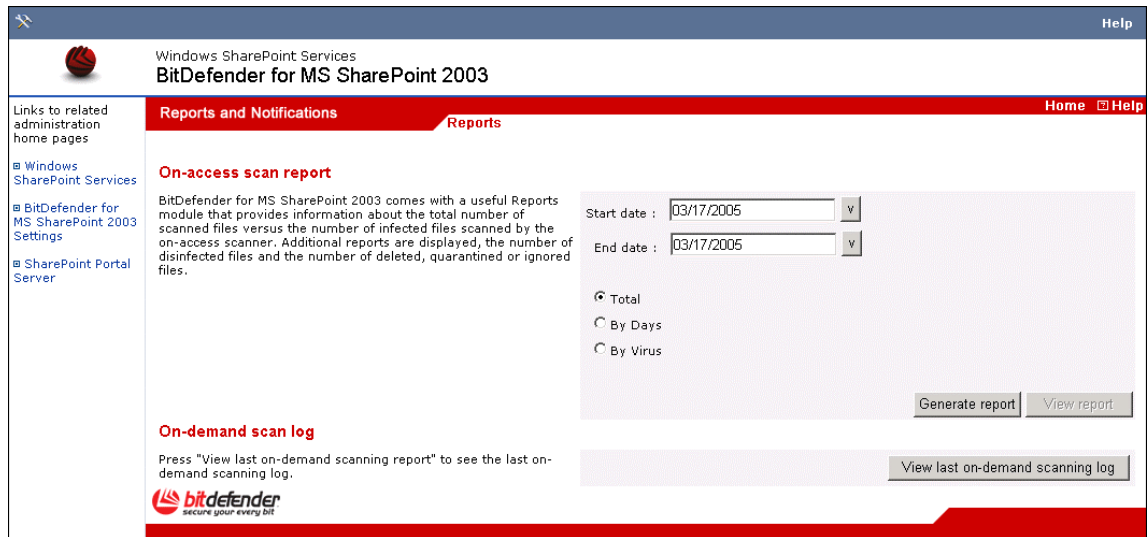


Figure 11

The module is divided in two sections:

- On-access scan report
- On-demand scan report

## Creating a scan report

In this section you can create report files concerning the on-access antivirus activity, during a period of time.

A report file contains the name of the scanned documents, their status (clean or infected), the virus names for the infected documents and the action BitDefender took on infected documents.

Steps to be followed in order to create report files:

- Select the time interval -**Start date** and **End date**;
- Select the report type - **Total**, **By Days** or **By Virus**);
- Click **Generate Report**. The new reports are located in `program files\common files\softwin\statistics\reports`;
- Click **View Report** to open the report file.

## Viewing a scan report

Click **View last on-demand scanning log** to open a report regarding the last on-demand scanning process (in the [On-demand scanner](#) module you can select the report options).

 **Note**

If no log file is present on your hard disk drive an error will appear: No on-demand scan report available or on-demand scan not yet performed.

# Real Time Virus Report

The module is customized on countries and allows sending alerts about the detected viruses to the BitDefender Lab. The reports will contain no confidential data, such as your name, IP address or others, and will not be used for commercial purposes.

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

To activate this feature you must access the **RTVR** module from the user interface (click **RTVR** from the **Reports & Notifications** section).

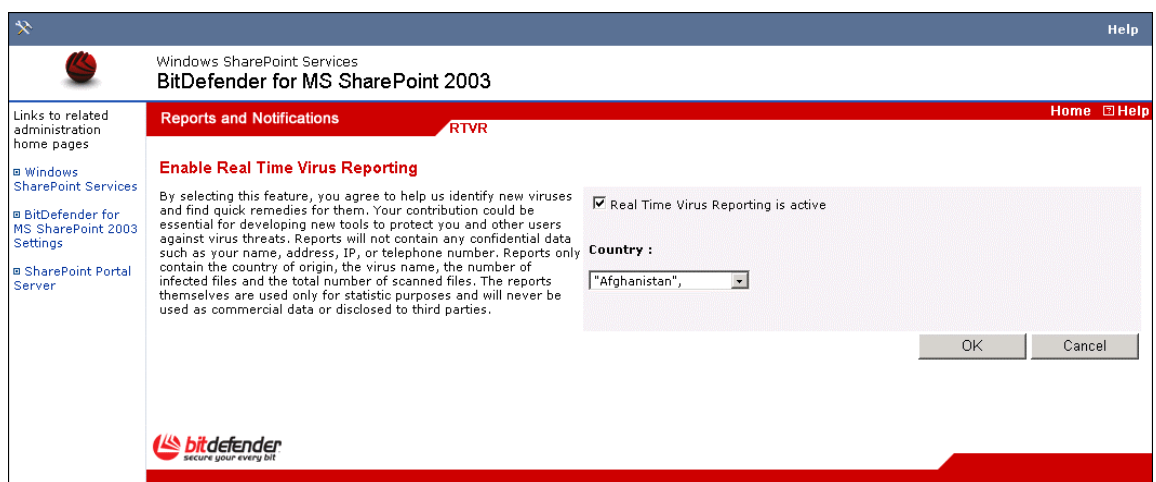


Figure 12

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

To see the statistic reports regarding the virus activity, follow the link:  
[http://www.bitdefender.com/bd/site/virusinfo.php?menu\\_id=2&dc=1&source=2](http://www.bitdefender.com/bd/site/virusinfo.php?menu_id=2&dc=1&source=2)

# Best practices

Steps to follow in order to ensure that all your document libraries from **MS SharePoint 2003** are free from viruses:

## 1. Register BitDefender

After the installation process is over, please [register](#) your **BitDefender for MS SharePoint 2003**.

## 2. Configure the update

Access the [Antivirus update](#) module and if you are using a proxy check **Use Proxy** and type in the settings. By default, BitDefender will automatically update every 8 hours. Click **Update now** to immediately update the scan engines.

## 3. Configure MS SharePoint Antivirus Settings

Enable the scan of upload&download documents from **Microsoft SharePoint** as described in the [On-access scanner](#) module.

## 4. Select the action to be taken on infected documents

Access the [Antivirus settings](#) section and select the desired action: disinfect, delete, move to Quarantine or ignore (no action). For disinfect you can select a second action in case the disinfection fails.

## 5. Enable BitDefender

Access the [On-access scanner](#) module and select the check box corresponding to **Configure MS Sharepoint AntiVirus settings**.

## 6. Verify that BitDefender is working with the EICAR test

The test consists in creating a file using a text editor, provided the file is saved in standard MS-DOS ASCII format and is 68 bytes long. It might also be 70 bytes if the editor puts a CR/LF at the end. The file must contain the following single line:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*.
```

Save the file to any name with COM extension, for example EICAR.COM an upload it to the MS SharePoint. BitDefender must treat this file as an infected document

### Note

The string must be reproduced on a single line.

### 7. Perform a full manual scan

Access the [On-demand scanner](#) module, click **All** and press the **Scan** button. A report file will be created in the [Reports&Logs](#) module.

### 8. Configure the Mail Notification module

If a virus is detected or an unexpected situation appears, there is the possibility of sending alarm messages by e-mail to the persons you designate. Access the [Mail Notification](#) module in order to configure BitDefender to send these notifications.

### 9. Create report files

From time to time create report files regarding the antivirus activity as described in the [Reports&Logs](#) module.

# Frequently Asked Questions

- 1. Q:** How can I tell if BitDefender is actually working?  
**A:** Use the EICAR test described in [Best practices](#) section.
- 2. Q:** How can I perform a manual scan?  
**A:** Access the [On-demand scanner](#) module, click **All** and press the **Scan** button. A report file will be created (click **log link** to open it)..
- 3. Q:** How can I disable BitDefender?  
**A:** Access the [On-demand scanner](#) module and clear the check box corresponding to **Enable SharePoint AntiVirus Integration**.
- 4. Q:** How can I set BitDefender to send mail notification in case a virus is found?  
**A:** Access the [Mail Notification](#) section and follow the instructions as described in this user guide.
- 5. Q:** What are the system requirements?  
**A:** The system requirements are:

  - Microsoft SharePoint Portal Server 2003 or
  - Microsoft Windows SharePoint Services v 2.0
- 6. Q:** How do I uninstall BitDefender?  
**A:** Follow the path: **Start** → **Programs** → **BitDefender for MS SharePoint** → **Repair & Uninstall** and in the window that will appear click the **Remove** button. This will start the uninstall process
- 7. Q:** How can I update BitDefender?  
**A:** By default, BitDefender will automatically update every 8 hours. But you can also update manually or change the time interval for the automatic update in the [Antivirus update](#) section.
- 8. Q:** Why is it necessary to update BitDefender scanning engines?  
**A:** Every time you perform an [update](#) new virus definitions will be added to the scan engines.
- 9. Q:** Where do I enter my serial number (license key)?  
**A:** You must access the [Register](#) section, type in the license key in the **Product ID** field and click **Register**.

# BitDefender Enterprise Manager Integration

## Description and features

**BitDefender Enterprise Manager** allows for full automation of routine tasks (including upgrades and updates), while letting the administrator install clients and execute tasks from anywhere in the network, in a safe and secure manner.

**BitDefender** introduces a new tool designed to facilitate administrative control over large networks. **BitDefender WMI Scripts v1.1 (Server Add-On)** implements tasks based on WMI (Windows® Management Instrumentation). These tasks can be executed across the BitDefender Enterprise Manager network. WMI server add-on is available with Enterprise v2.5.

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

### The top solution for complex networks security

- 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 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

### **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 centralized multi-platform integrated installation.

### **Remote management**

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

### **Fast, Free Live! Updates**

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

### **Completely automated response to new virus outbreaks**

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

### **Unlimited Scalable Solution**

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

### **Remote Management**

Management is available from any network connected system, drastically reducing the reaction time to any incident.

### **Intelligent Alerts**

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

## Supported clients

**BitDefender Enterprise Manager v2.5** 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  
BitDefender v1.6 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)

## How does it work?

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

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

## Working schema

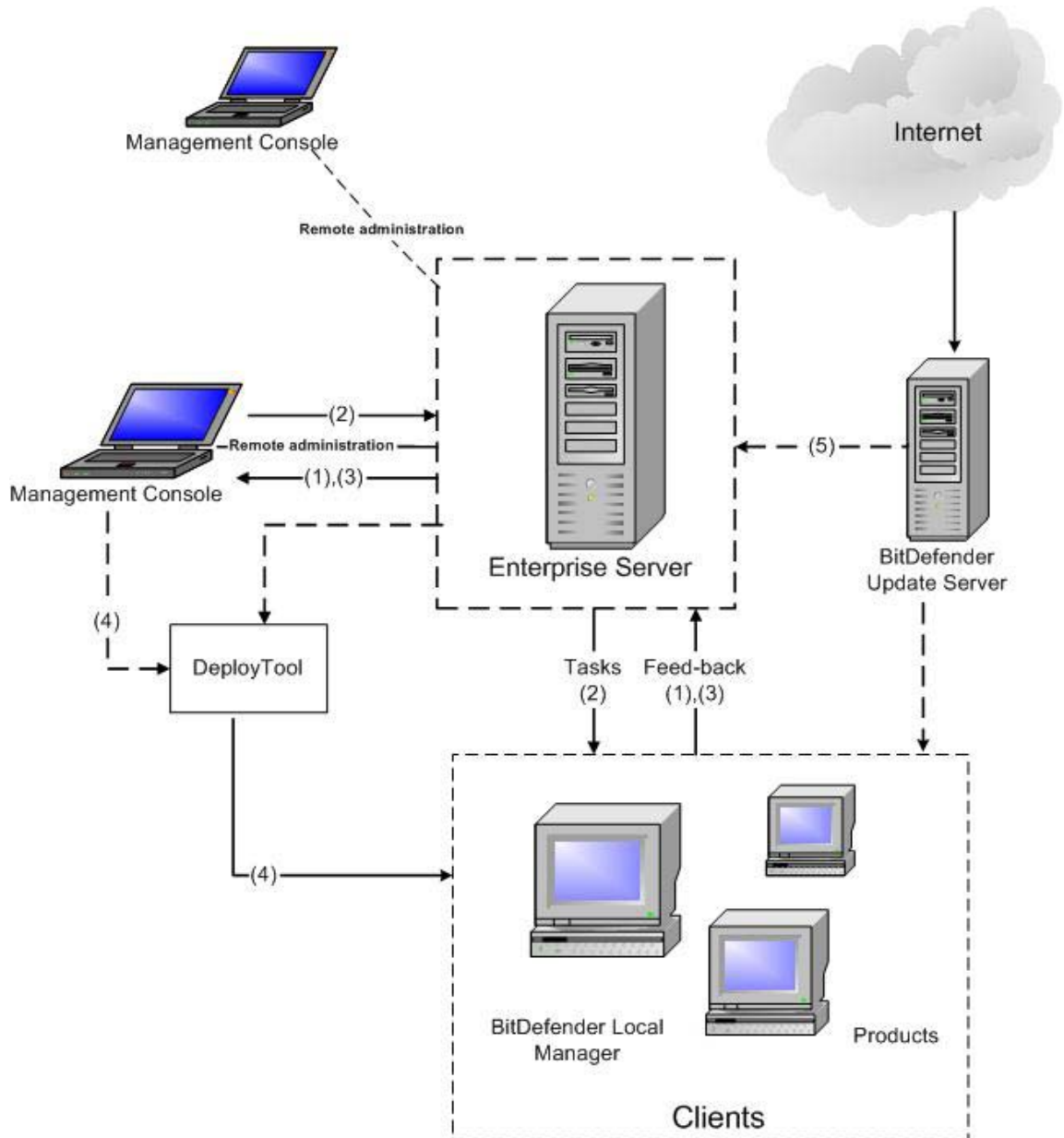


Figure 13

**BitDefender Enterprise Manager** is divided into several parts: [BitDefender Server](#), [BitDefender Local Manager](#), [BitDefender Management Console](#), [BitDefender Deployment Tool](#) and [BitDefender Update Server](#).

From the scheme it can be observed that five information flows can be identified and they can be described as follows:

1. **BitDefender Deployment Tool** sends the task to install **BitDefender Local Manager** to the workstations.
2. **BitDefender Local Manager** creates a database with all the BitDefender products already installed on the workstations and then sends the information to the **BitDefender Server**. The Server takes it over and sends it to 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 **BitDefender Server** and

forwarded to the **BitDefender Local Manager** corresponding to each workstation. Further on, BitDefender products will execute the commands selected by the user through the management console.

4. The results of the commands' execution on the workstations are sent to the **BitDefender Server**. Depending on the user's option, this information is used for creating reports that can be viewed through the management console.
5. **BitDefender Update Server** sets up an upgrade location within your local network, in a folder that must be 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**. The users from the client workstations can also choose to update their antivirus product from this location.

**TIP:** You can publish the downloads folder by using **BitDefender HTTP Server** or another HTTP server like IIS or Apache.

## BitDefender Server

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

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

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.

### Note

To manage the BitDefender clients from a different workstation than the **BitDefender Server**, you must perform a custom installation of the **BitDefender Enterprise**. In the third step of the installation click **Custom** and in the window that appears disable all other components than **BitDefender Enterprise Management Console** and **BitDefender Deployment Tool**.

### System requirements:

- **Processor:** Intel Pentium Compatible processor - 200 MHz or higher
- **Minimum hard disk space:** 100MB
- **Minimum RAM Memory:** 64MB
- **Operating system:** Windows NT SP6, Windows 2000, Windows XP or 2003

## BitDefender Local Manager

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

### System requirements:

- **Processor:** Intel Pentium Compatible processor
- **Minimum hard disk space:** 10MB
- **Minimum RAM Memory:** 32MB
- **Operating system:** minimum Windows 98 SE

## BitDefender Management Console

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

- ➔ Easily administrate of 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 from the network;
- ➔ Schedule tasks like: 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 the workstations or whenever an error occurs;
- ➔ Create and display different reports and statistics.

### Note

To install only the management console on a workstation you must perform a custom installation of the **BitDefender Enterprise**. In the third step of the installation, click **Custom** and in the window that appears disable all other components than **BitDefender Enterprise Management Console**.

**TIP:** If you do not want to install the **BitDefender Management Console** on your system, but still desire to gain access to the **BitDefender Server**, you can use the **Terminal Services Console (Remote Desktop Connection)** to connect to the workstation that has installed the **BitDefender Management Console** and then work normally.

### System requirements:

- **Processor:** Intel Pentium Compatible processor
- **Minimum hard disk space:** 10MB
- **Minimum RAM Memory:** 64MB
- **Operating system:** Windows NT SP6, Millennium, 2000, XP or 2003
- Display with minimum resolution of 800x600 / 16 bit
- Internet Explorer 5.0 or superior



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

## BitDefender Deployment Tool

This is a component independent of all the others. It allows the remote installation of the **BitDefender Local Manager**, eliminating the necessity 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.

**TIP:** You can put it on a cd, on a shared folder, send it by e-mail or use a logon script in order to install it on the workstations.

### System requirements:

- **Operating system:** Windows NT SP6, 2000, XP or 2003
- Internet Explorer 5.5 or higher

## 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.



You must publish the folder where you download the updates by using **BitDefender HTTP Server** or another HTTP server like IIS or Apache.

### System requirements:

- **Processor:** Intel Pentium Compatible processor
- **Minimum hard disk space:** 100MB (for updates)
- **Minimum RAM Memory:** 64MB
- **Operating system:** Windows NT SP6, 2000, XP or 2003
- Internet Explorer 5.0 or higher

### Note

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

# Additional Task Templates

**BitDefender for MS SharePoint 2003** deeply integrates with BitDefender Enterprise Manager, meaning you can configure this product from the Enterprise Management Console.

 **Note**

The **BitDefender for MS SharePoint 2003** must be installed on a BitDefender Enterprise client. This means **BitDefender Local Manager** is already installed on that workstation or it will be installed in order to import the newly created tasks from that workstation.

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 SharePoint 2003** installed and from the **Clients&Groups** menu, point **Clients**, click **Import Tasks Templates from Selected Clients**.

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

- 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**.

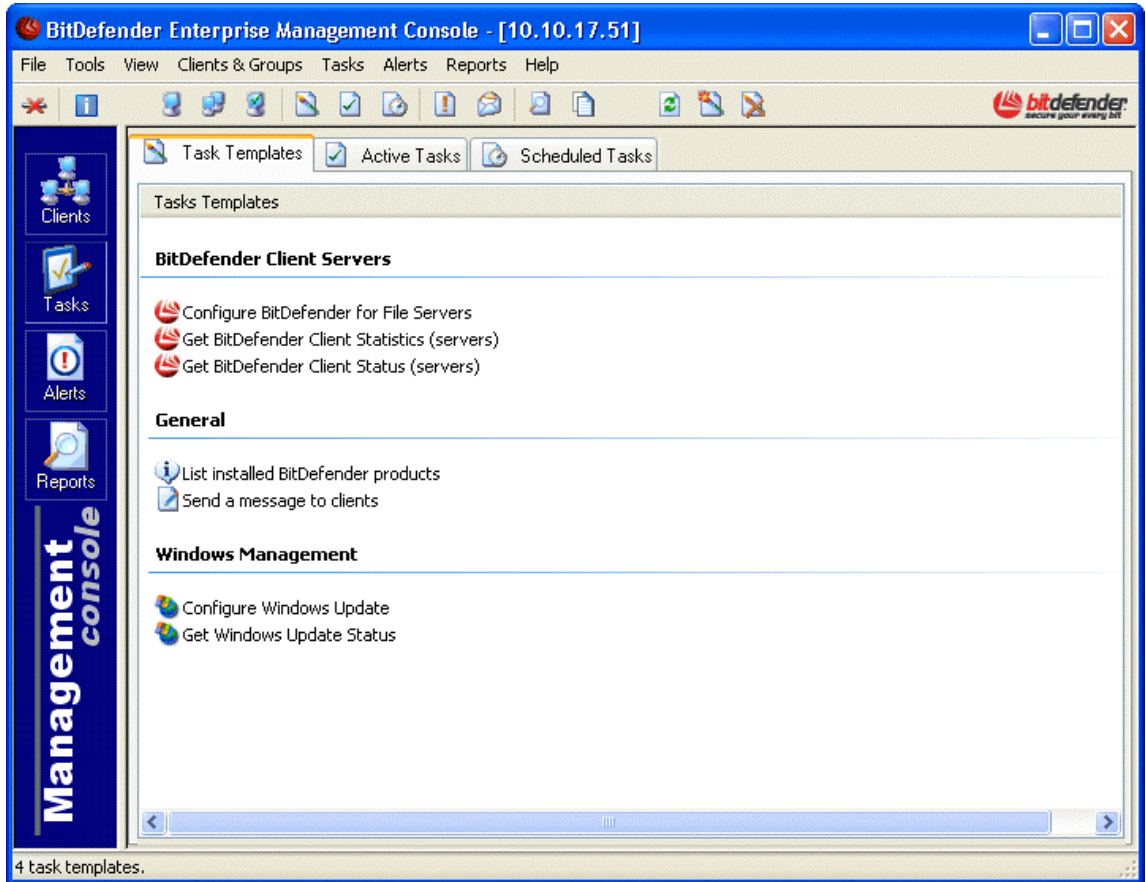







Figure 14

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



### BitDefender Client Servers

-  [Configure BitDefender for MS SharePoint 2003](#) – to configure **BitDefender for MS SharePoint 2003**;
-  [Get BitDefender Client Statistics](#) - to receive statistics about the antivirus product.
-  [Get BitDefender Client Status](#) - to receive information about the antivirus status.


### General

-  [List installed BitDefender products](#) - to show a list with all the BitDefender products installed on the selected workstations;
-  [Send a message to clients](#) - to receive information about the windows update status on specified clients.

### Windows Management

-  [Configure Windows Update](#) - to configure the update of windows on specified clients;
-  [Get Windows Update Status](#) - to send a message to specified clients.

## Configuring BitDefender for MS SharePoint 2003

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

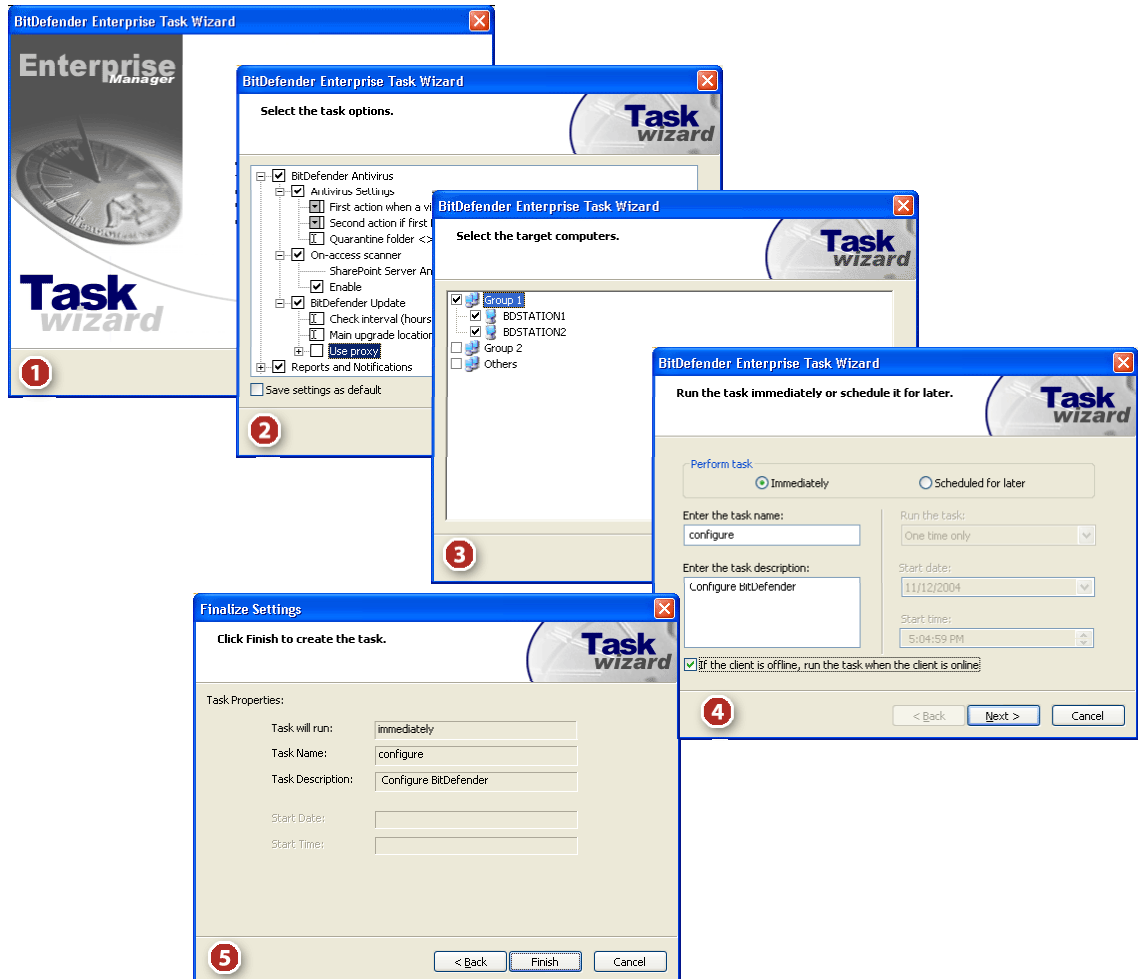


Figure 15

Configuration steps:

1. Click **Next** in order to continue or click **Cancel** if you want to quit configuration.
2. Here you can configure the **BitDefender for MS SharePoint 2003**. The configuration options are grouped in three categories: **BitDefender Antivirus**, **Reports and Notifications** and **BitDefender Information**.

### Note

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

## BitDefender Antivirus

Select the check box corresponding to **BitDefender Antivirus** in order to configure BitDefender. Three categories of options are available: **Antivirus Settings**, **On-access scanner** and **BitDefender Update**.

### Antivirus Settings

Select the check box corresponding to the **Antivirus Settings** category in order to enable this category of options.

- ➔ Click the arrow corresponding to **First action when a virus is found** and select from the list the first action on infected objects. BitDefender allows selecting two actions in case an infected object is found. The second action is enabled only in case the first action you selected is to disinfect the infected objects.

You can select one of the following actions:

First action	Description
Ignore	In this case the infection is ignored and no action will be taken on the infected document.
Disinfect	To disinfect the infected document.
Delete	To delete the infected document.
Move to quarantine	To move the infected document to the quarantine.

- ➔ Click the arrow corresponding to **Second action to take when first fails** and select from the list the second action on the infected files. This option is enabled only if the first action selected is **Disinfect**.

The following options are available.

Second action	Description
Ignore	In this case the infection is ignored and no action will be taken on the infected document.
Delete	When the disinfection fails, the infected document is immediately deleted.
Move to quarantine	When the disinfection fails, the infected document is immediately moved to quarantine.

**TIP:** We recommend using 1<sup>st</sup> action: **Disinfect**, 2<sup>nd</sup> action: **Delete**.

- ➔ In case the isolation of the infected documents in the quarantine area was selected, it must be specified the complete path to the quarantine folder. For this click the **Quarantine folder** field and type in the path to the quarantine.

The quarantine folder must be previously created and must be located on the server. The complete path must be specified.

For example: `C:\quarantine`

### On-access scanner

Select the check box corresponding to **Enable** to activate the antivirus protection on your SharePoint Server.

### BitDefender Update

Select the check box corresponding to **BitDefender Update** in order to enable this category of options. The following options are available:

- **Check interval** - BitDefender allows the selection of the update checking interval. By default this is 8 hours. If you want to change it, type in a new interval.
- **Update 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.

## Reports and Notifications

Select the check box corresponding to **Reports and Notifications** in order to configure BitDefender. Two categories of options are available: **Mail Notification** and **Real Time Virus Report**.

### Mail Notification

Select the check box corresponding to **Enable** to activate the mail notification module.

In order to send alerts via e-mail you must first specify some information:

- **SMTP Server** - type in the name of the SMTP server that the company uses to send messages;
- **From Address** - type in the e-mail address that will appear in the sender field;



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.

- **Notify on Virus** - type in the person's e-mail address you want to be notified in case a virus is found;
- **Notify on Warning** - type in the person's e-mail address you want to be notified in case a special situation, such as disabling the BitDefender protection, appears;

→ **Notify on Error** - type in the person's e-mail address you want to be notified when a disfunctionality of BitDefender appears. Such situations may occur, for example, because of the accidental deletion of some files or failure to load the antivirus engines;

**TIP:** If you want to send messages to more than just one mail recipient, these addresses must be separated by “;”.

### Real Time Virus Report

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

## BitDefender Information

Select the check box corresponding to **BitDefender Information** in order to register BitDefender. Check **Register** and type in the serial number in the **Registration Key** field.

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

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

**TIP:** If a group contains at least one client then a double-click on that group's name or its corresponding icon will expand that group.

You can choose to run the task on one or several clients. To select all the clients from a group select the check box corresponding to that group's name.



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

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

4. 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.



The task may fail if the target workstation is offline, therefore select the check box corresponding to **If a client is offline, run the task when the client is online**.

**TIP:** The task may fail if the target workstation is offline, therefore select the check box corresponding to **If a client is offline, run the task when the client is online**.

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

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

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


**TIP:** The task may fail if the target workstation is offline, therefore select the check box corresponding to **If a client is offline, run the task when the client is online**.

Click **Next**.

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

Click **Finish**. Depending on the run time you have selected, the task will appear in the **Active Tasks** section, in case it is an immediate task or in the **Scheduled Tasks** section, if it is a scheduled task.

## Retrieving BitDefender statistics

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

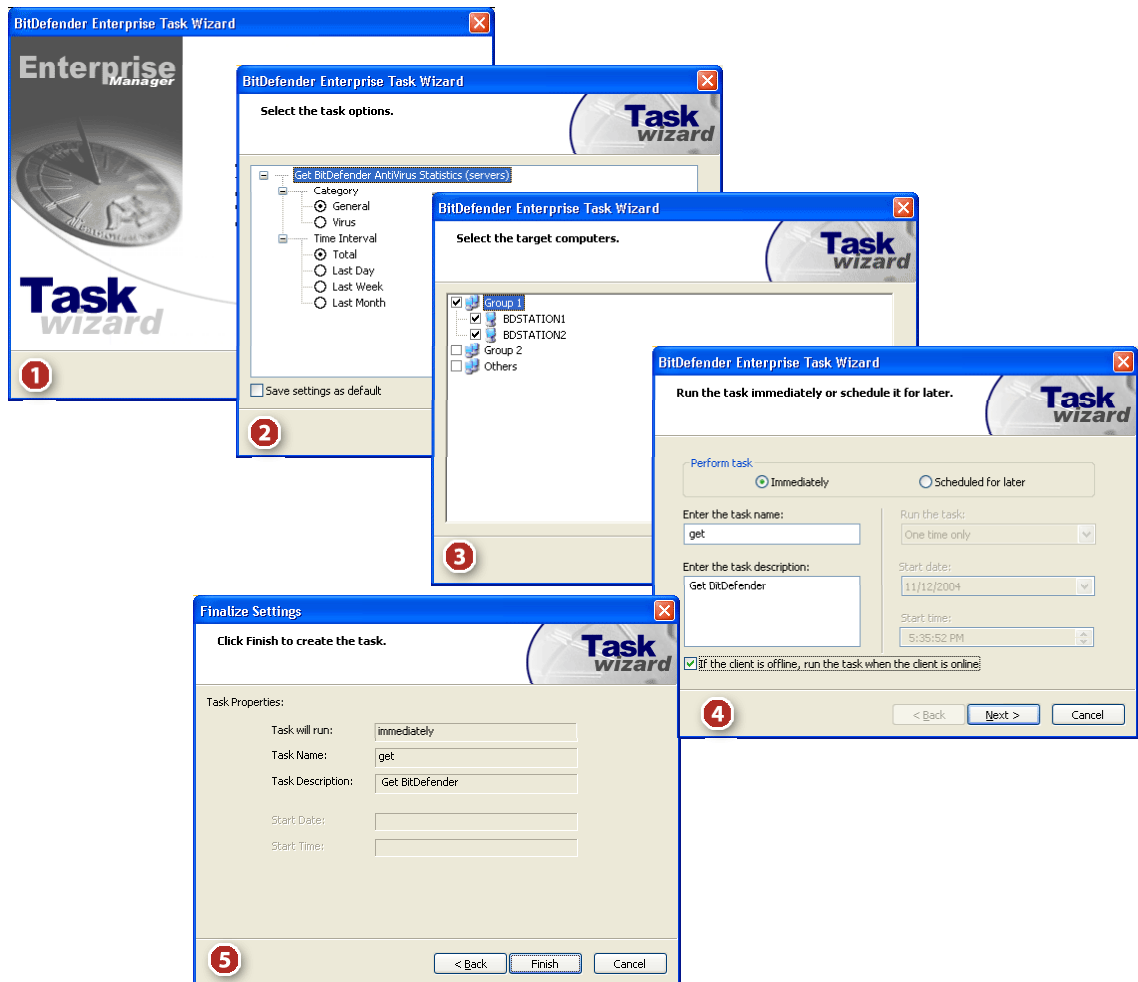


Figure 16

Wizard steps:

1. Click **Next** in order to continue or click **Cancel** if you want to quit.
2. Select the category (**General** or **Virus**) and the time interval (**Total**, **Last Day**, **Last Week** or **Last Month**) and click **Next**.

**TIP:** 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.

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

**TIP:** If a group contains at least one client then a double-click on that group's name or its corresponding icon will expand that group.

You can choose to run the task on one or several clients. To select all the clients from a group select the check box corresponding to that group's name.



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

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

4. 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.

**TIP:** The task may fail if the target workstation is offline, therefore select the check box corresponding to **If a client is offline, run the task when the client is online**.

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

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

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




The task may fail if the target workstation is offline, therefore select the check box corresponding to **If a client is offline, run the task when the client is online**.

Click **Next**.

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

Click **Finish**. Depending on the run time you have selected, the task will appear in the **Active Tasks** section, in case it is an immediate task or in the **Scheduled Tasks** section, if it is a scheduled task.

## Retrieving BitDefender status

In order to obtain the BitDefender status of the selected servers, you must 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:

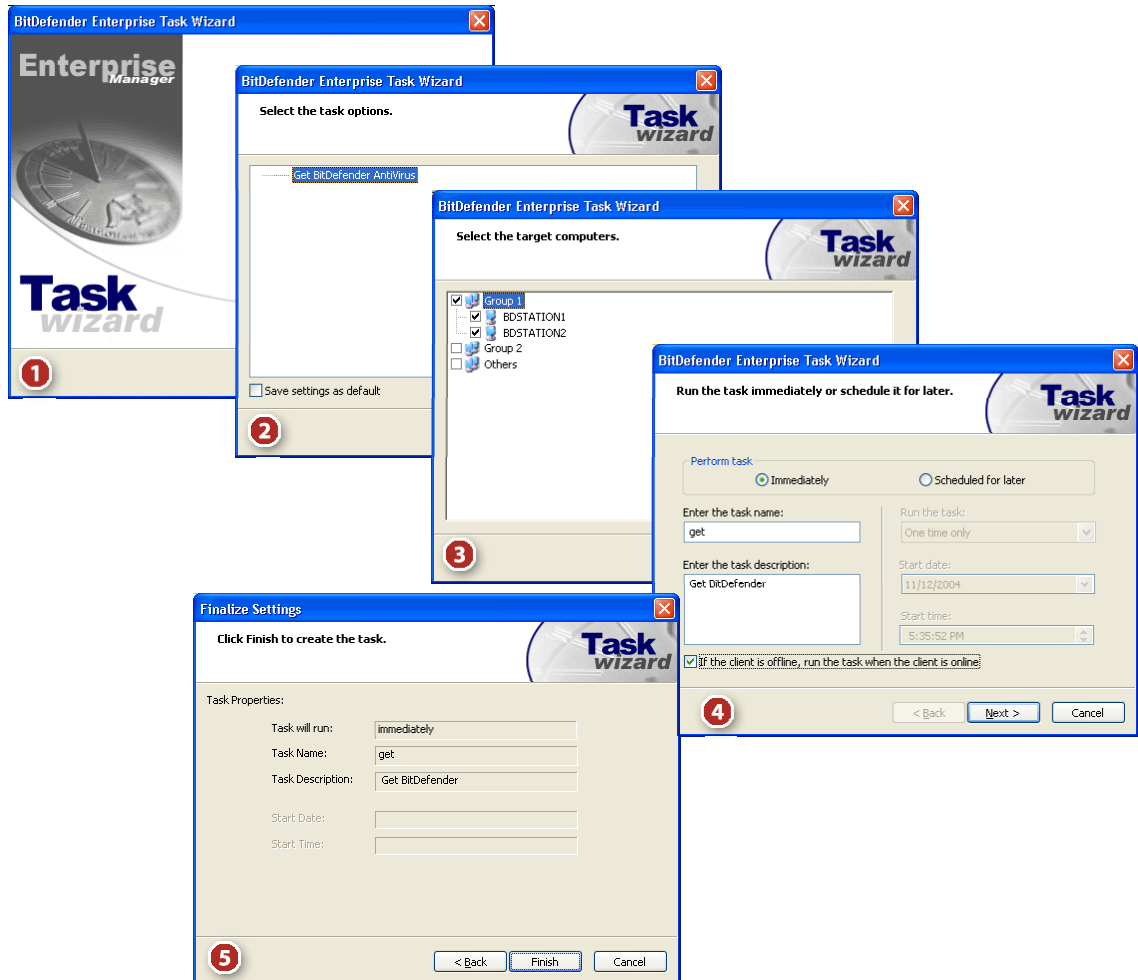


Figure 17

Wizard steps:

1. Click **Next**.
2. Select the components you want to receive information about and click **Next**.
3. You must select the clients and/or the groups.

**TIP:** If a group contains at least one client then a double-click on that group's name or its corresponding icon will expand that group.

You can choose to run the task on one or several clients. To select all the clients from a group select the check box corresponding to that group's name.



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

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

4. You can opt for an immediate or a programmed task.

For an immediate task, click **Immediately** and specify the following:

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

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

- **Enter the task name** - type in a name for the task;
- **Enter the task description** - type in a short description of the task;
- **Run the task** - it is a list with time intervals when the task should run.

**One time only** - to run the task on the selected clients only once at a specified moment;

**Every hour** - to run the task on the selected clients every hour;

**Every 6 hours** - to run the task on the selected clients at every 6 hours;

**Every 12 hours** - to run the task on the selected clients at every 12 hours;

**Every day** - to run the task on the selected clients daily;

**Every two days (48 hours)** - to run the task on the selected clients at every 2 days;

**Every three days (72 hours)** - to run the task on the selected clients at every 3 days;

**Weekly** - to run the task on the selected clients weekly;

**Monthly** - to run the task on the selected clients monthly.

- **Start date** - click the arrow corresponding to the field and select a day from the calendar that appears;
- **Start time** - type the hour when the task will launch. You can use the corresponding arrows up/down.




The task may fail if the target workstation is offline, therefore select the check box corresponding to **If a client is offline, run the task when the client is online**.

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

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

Click **Finish**. Depending on the run time you have selected, the task will appear in the **Active Tasks** section, in case it is an immediate task or in the **Scheduled Tasks** section, if it is a scheduled task.

## Retrieving a list with all BitDefender products installed

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

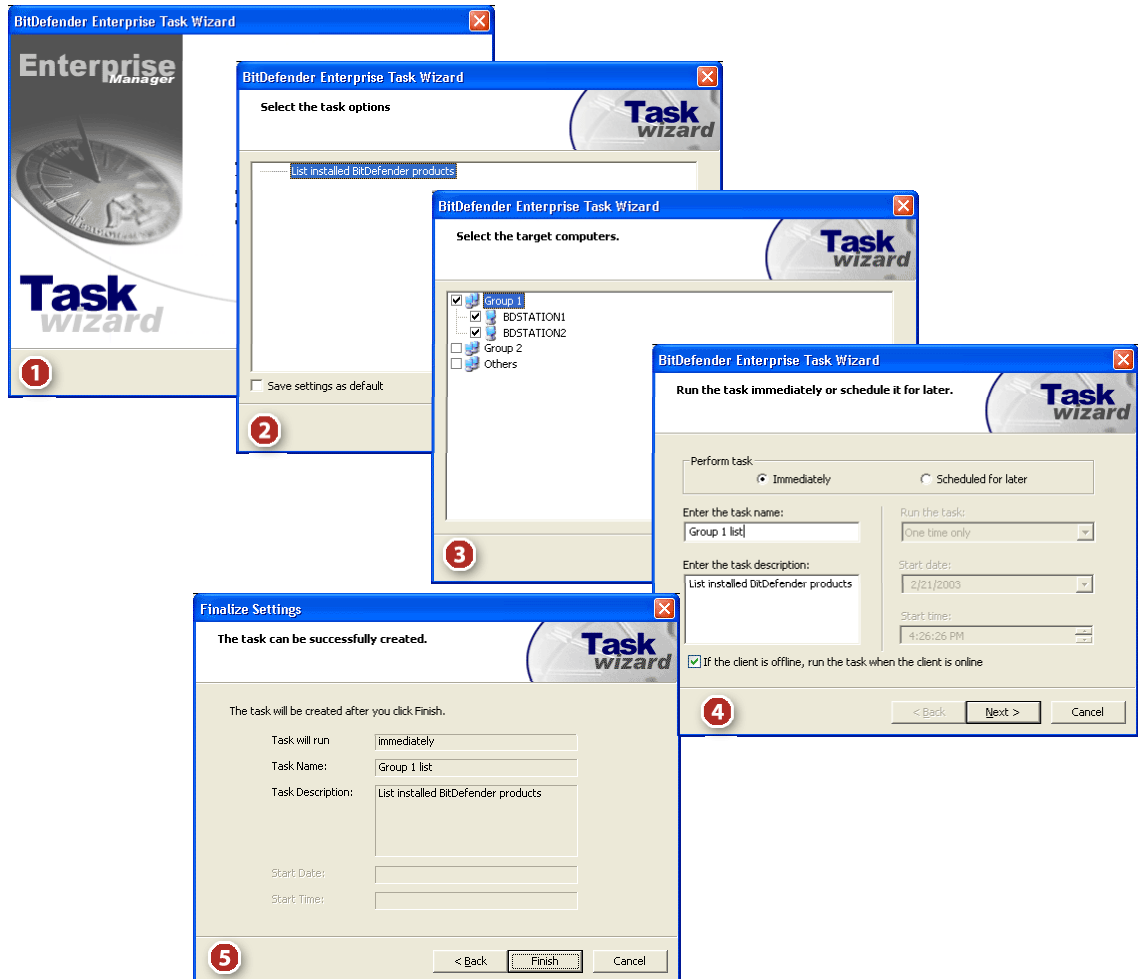


Figure 18

Wizard steps:

1. Click **Next**.
2. Click **Next**.
3. You must select the clients and/or the groups.

**TIP:** If a group contains at least one client then a double-click on that group's name or its corresponding icon will expand that group.

You can choose to run the task on one or several clients. To select all the clients from a group select the check box corresponding to that group's name.



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

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

**4.** You can opt for an immediate or a programmed task.

For an immediate task, click **Immediately** and specify the following:

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

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

- **Enter the task name** - type in a name for the task;
- **Enter the task description** - type in a short description of the task;
- **Run the task** - it is a list with time intervals when the task should run.

**One time only** - to run the task on the selected clients only once at a specified moment;

**Every hour** - to run the task on the selected clients every hour;

**Every 6 hours** - to run the task on the selected clients at every 6 hours;

**Every 12 hours** - to run the task on the selected clients at every 12 hours;

**Every day** - to run the task on the selected clients daily;

**Every two days (48 hours)** - to run the task on the selected clients at every 2 days;

**Every three days (72 hours)** - to run the task on the selected clients at every 3 days;

**Weekly** - to run the task on the selected clients weekly;

**Monthly** - to run the task on the selected clients monthly.

- **Start date** - click the arrow corresponding to the field and select a day from the calendar that appears;
- **Start time** - type the hour when the task will launch. You can use the corresponding arrows up/down.




The task may fail if the target workstation is offline, therefore select the check box corresponding to **If a client is offline, run the task when the client is online**.

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

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

Click **Finish**. Depending on the run time you have selected, the task will appear in the **Active Tasks** section, in case it is an immediate task or in the **Scheduled Tasks** section, if it is a scheduled task..

## Sending a message to clients

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

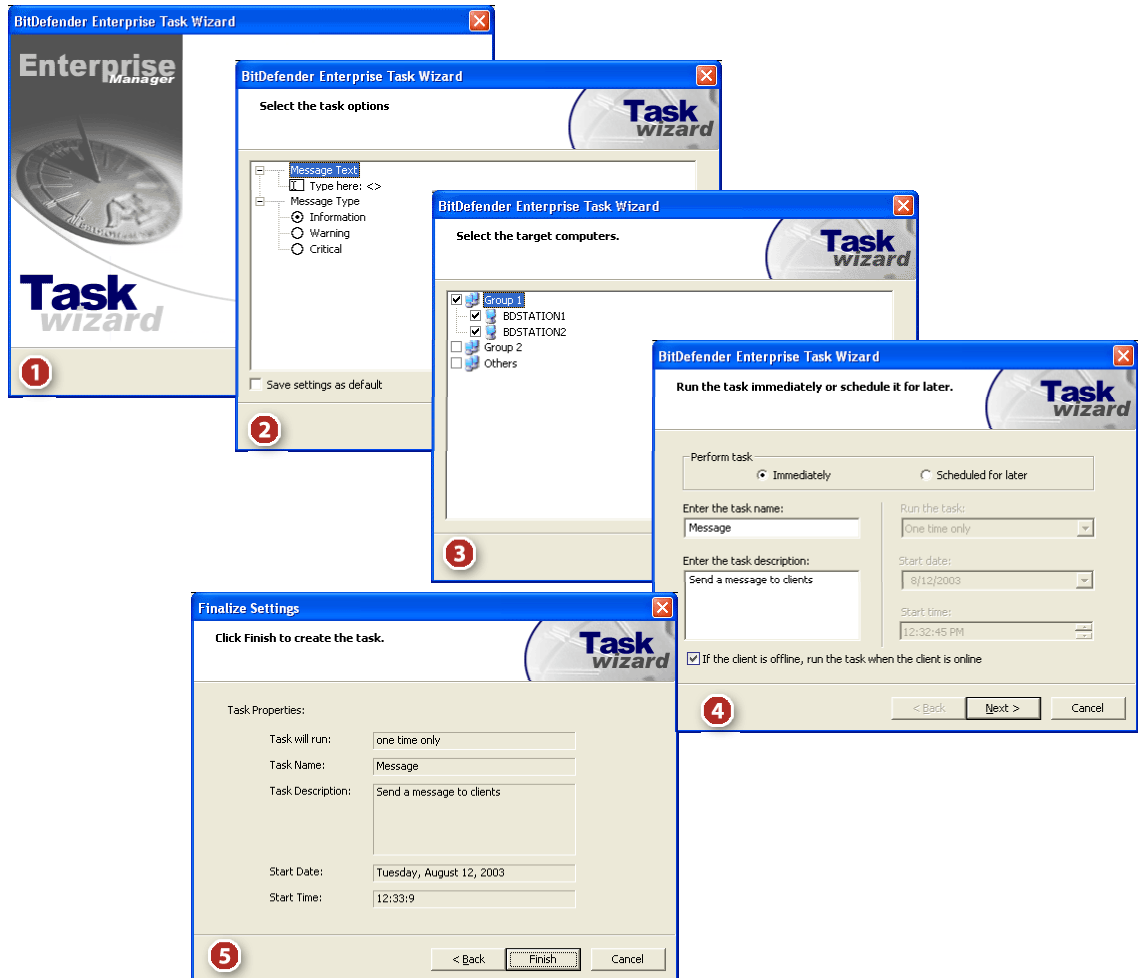


Figure 19

Wizard steps:

1. Click **Next**.
2. Click the **Type here** field and introduce the message you want to send.

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

Select the check box corresponding to **Save settings as default** to keep the same configuration for the future tasks. Click **Next**.

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

**TIP:** If a group contains at least one client then a double-click on that group's name or its corresponding icon will expand that group.

You can choose to run the task on one or several clients. To select all the clients from a group select the check box corresponding to that group's name.



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

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

**4.** You can opt for an immediate or a programmed task.

For an immediate task, click **Immediately** and specify the following:

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

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

- **Enter the task name** - type in a name for the task;
- **Enter the task description** - type in a short description of the task;
- **Run the task** - it is a list with time intervals when the task should run.

**One time only** - to run the task on the selected clients only once at a specified moment;

**Every hour** - to run the task on the selected clients every hour;

**Every 6 hours** - to run the task on the selected clients at every 6 hours;

**Every 12 hours** - to run the task on the selected clients at every 12 hours;

**Every day** - to run the task on the selected clients daily;

**Every two days (48 hours)** - to run the task on the selected clients at every 2 days;

**Every three days (72 hours)** - to run the task on the selected clients at every 3 days;

**Weekly** - to run the task on the selected clients weekly;

**Monthly** - to run the task on the selected clients monthly.

- **Start date** - click the arrow corresponding to the field and select a day from the calendar that appears;
- **Start time** - type the hour when the task will launch. You can use the corresponding arrows up/down.




The task may fail if the target workstation is offline, therefore select the check box corresponding to **If a client is offline, run the task when the client is online**.

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

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

Click **Finish**. Depending on the run time you have selected, the task will appear in the **Active Tasks** section, in case it is an immediate task or in the **Scheduled Tasks** section, if it is a scheduled task.

## Configuring Windows Update

To configure the windows update on clients, you must double-click the  **Configure Windows Update** icon.

This will launch the wizard, which will guide you through the configuration process.

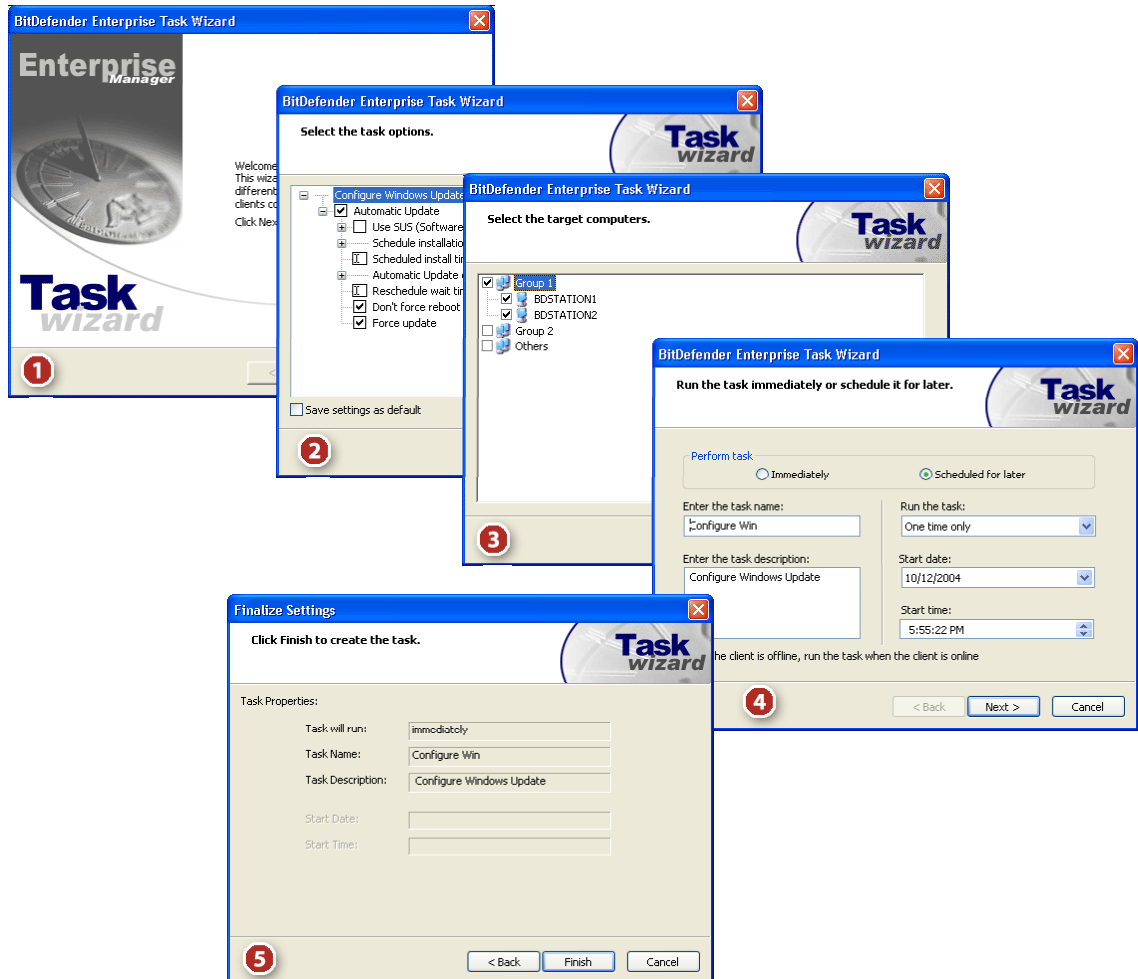


Figure 20

Configuration steps:

1. Click **Next**.
2. Click the **Type here** field and introduce the message you want to send.

Select **Automatic Update** to access the configuration settings. These settings are grouped in three main categories (**SUS Server options**, **Schedule options** and **Automatic Update options**) and three other options.

### Note

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

## SUS Server options

Select the check box corresponding to **Use SUS Server** in order to enable this feature. Type the SUS server address and the statistics server address in the corresponding fields.



If don't select this option then default Windows update location will be used.

## Schedule options

Select the day and the hour when the server will check for windows updates. You can select to verify every day or a specified day from the week.

## Automatic Update options

You can select to notify the local administrator before downloading any updates and / or before installing them. If you don't want to notify him select the third option.

## Other options

→ **Reschedule wait time** - to set the reschedule wait time. Two situations are possible.

- If a scheduled installation is missed (because the client computer was turned off) and **Reschedule wait time** is not set to a value between 1 and 60, **Automatic Updates** waits until the next scheduled day and time to perform the installation.
- If a scheduled installation is missed and **Reschedule wait time** is set to a value between 1 and 60, then **Automatic Updates** reschedules the installation to occur at the **Automatic Updates** service start time plus the number of minutes specified in **Reschedule wait time**.

→ **Don't force reboot** - to offer the logged on users the possibility to choose not to restart the system.

→ **Force Update** - to check for updates in the following minutes.

Select the check box corresponding to **Save settings as default** to keep the same configuration for the future tasks. Click **Next**.

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

**TIP:** If a group contains at least one client then a double-click on that group's name or its corresponding icon will expand that group.

You can choose to run the task on one or several clients. To select all the clients from a group select the check box corresponding to that group's name.



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

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

4. You can opt for an immediate or a programmed task.

For an immediate task, click **Immediately** and specify the following:

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

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

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



The task may fail if the target workstation is offline, therefore select the check box corresponding to **If a client is offline, run the task when the client is online**.

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

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

Click **Finish**. Depending on the run time you have selected, the task will appear in the **Active Tasks** section, in case it is an immediate task or in the **Scheduled Tasks** section, if it is a scheduled task.

## Retrieving Windows Update status

To obtain the windows update status on selected clients, you must double-click the **Get Windows Update Status** icon.

This will launch the wizard, which will guide you through the task.

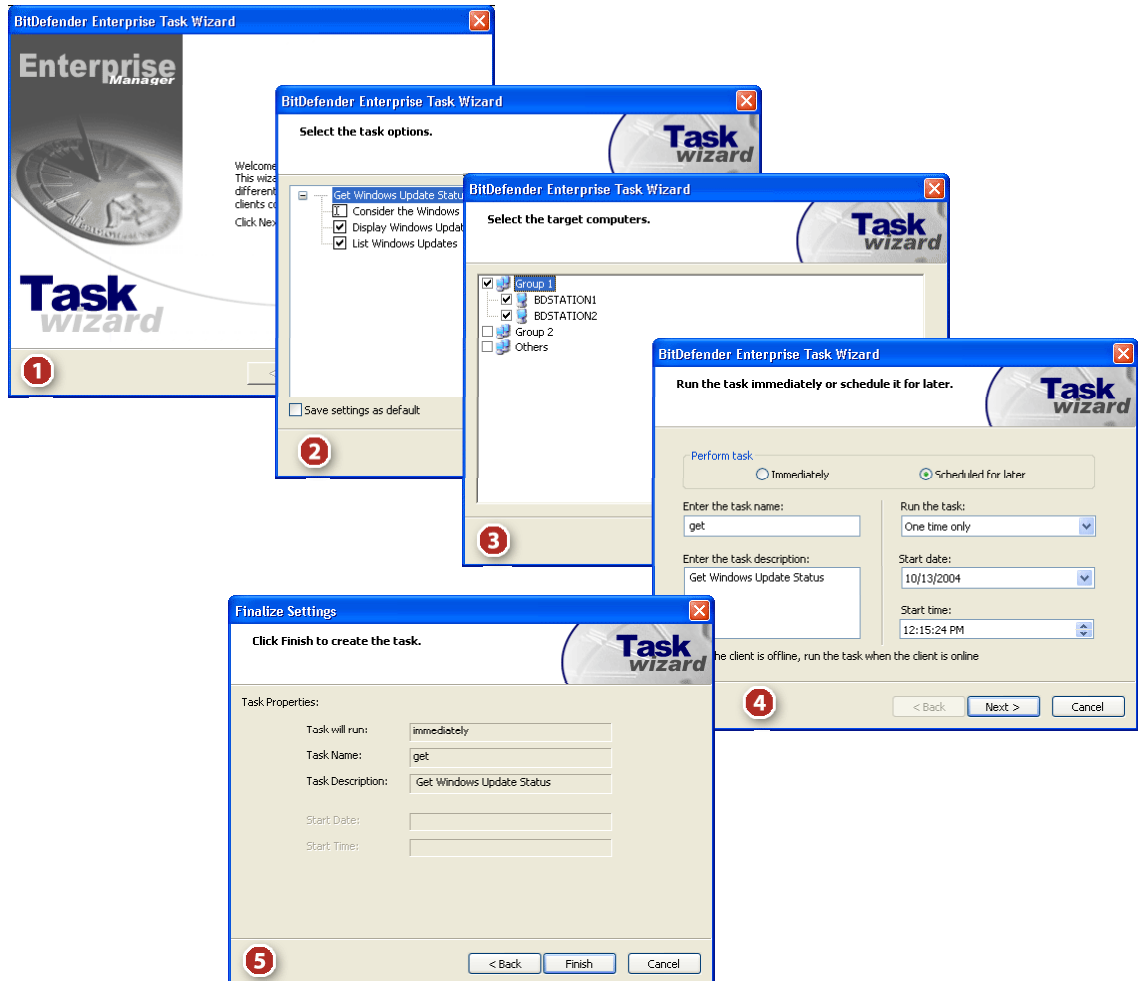



Figure 21

Wizard steps:

1. Click **Next**.
2. You have three options:
  - ➔ **Consider the Windows updates obsolete after x days** - to consider a client not updated after x days;
  - ➔ **Display Windows Updates settings** - to see in the task result the Windows Update settings;
  - ➔ **List Windows Updates** - to see in the task result a list with all windows updates on each client.



You can see only what updates have been made on target computers. The task will not compare those to the ones from the Microsoft server. The task result can be seen in the bottom side of the **Active Task** section.

**TIP:** In order to find for how many days a computer was not updated to windows you must create a report. After that you can use the **Resolve issues**  button to launch an update task.

Select the check box corresponding to **Save settings as default** to keep the same configuration for the future tasks. Click **Next**.

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

**TIP:** If a group contains at least one client then a double-click on that group's name or its corresponding icon will expand that group.

You can choose to run the task on one or several clients. To select all the clients from a group select the check box corresponding to that group's name.



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

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

### 4. You can opt for an immediate or a programmed task.

For an immediate task, click **Immediately** and specify the following:

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

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

- **Enter the task name** - type in a name for the task;
- **Enter the task description** - type in a short description of the task;
- **Run the task** - it is a list with time intervals when the task should run.

**One time only** - to run the task on the selected clients only once at a specified moment;

**Every hour** - to run the task on the selected clients every hour;

**Every 6 hours** - to run the task on the selected clients at every 6 hours;

**Every 12 hours** - to run the task on the selected clients at every 12 hours;

**Every day** - to run the task on the selected clients daily;

**Every two days (48 hours)** - to run the task on the selected clients at every 2 days;

**Every three days (72 hours)** - to run the task on the selected clients at every 3 days;

**Weekly** - to run the task on the selected clients weekly;

**Monthly** - to run the task on the selected clients monthly.

- **Start date** - click the arrow corresponding to the field and select a day from the calendar that appears;
- **Start time** - type the hour when the task will launch. You can use the corresponding arrows up/down.



The task may fail if the target workstation is offline, therefore select the check box corresponding to **If a client is offline, run the task when the client is online**.

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

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

Click **Finish**. Depending on the run time you have selected, the task will appear in the **Active Tasks** section, in case it is an immediate task or in the **Scheduled Tasks** section, if it is a scheduled task.

# Contact information

As a valued provider, SOFTWIN strives to provide its customers an unparalleled level of fast and accurate support. The Support Center is continually updated with the newest virus descriptions and answers to common questions to help you find answers to your problems in a timely manner.

We at SOFTWIN, are dedicated to saving customer's time and money by providing the most advanced products at the fairest prices. We think that a successful business has a lot to do with good communication and a commitment to excellence in customer support.

Sales department: [sales@bitdefender.com](mailto:sales@bitdefender.com)  
<http://buy.bitdefender.com>

Technical support: [support@bitdefender.com](mailto:support@bitdefender.com)

Phone: 0040-21-233 07 80

Product web site: [www.bitdefender.com](http://www.bitdefender.com)

Address:

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

Please send feedback regarding the document to: [documentation@bitdefender.com](mailto:documentation@bitdefender.com)