bitdefender
Mobile Security

User's guide

Antivirus

bitdefender
secure your every bit

BitDefender Mobile Security

User's guide

BitDefender

Published 2007.02.05
Version 2.0

Legal Notice


bitdefender
secure your every bit

Table of Contents

License and Warranty

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

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

This License Agreement is a legal agreement between you (either an individual or a legal person) and SOFTWIN for use of SOFTWIN's software product identified above, which includes software and services, and may include associated media, printed materials, and "online" or electronic documentation (hereafter designated as "BitDefender"), all of which are protected by international copyright laws and international treaties. By installing, copying or using BitDefender, you agree to be bound by the terms of this agreement.

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

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

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

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

USER LICENSE. This license applies to BitDefender software that can be installed on a single device (Smartphone, PDA or other similar hardware) and which does not provide network services. Each primary user may install this software on a single device and may make one additional copy for backup on a different device. The number of primary users allowed is the number of the users of the license.

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

EXPIRATION. The product will cease to perform its functions immediately upon expiration of the license.

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

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

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

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, SOFTWIN DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE PRODUCTS, ENHANCEMENTS, MAINTENANCE OR SUPPORT RELATED THERETO, OR ANY OTHER MATERIALS (TANGIBLE OR INTANGIBLE) OR SERVICES SUPPLIED BY HIM. SOFTWIN HEREBY EXPRESSLY DISCLAIMS ANY IMPLIED WARRANTIES AND CONDITIONS, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A

PARTICULAR PURPOSE, TITLE, NON INTERFERENCE, ACCURACY OF DATA, ACCURACY OF INFORMATIONAL CONTENT, SYSTEM INTEGRATION, AND NON INFRINGEMENT OF THIRD PARTY RIGHTS BY FILTERING, DISABLING, OR REMOVING SUCH THIRD PARTY'S SOFTWARE, SPYWARE, ADWARE, COOKIES, EMAILS, DOCUMENTS, ADVERTISEMENTS OR THE LIKE, WHETHER ARISING BY STATUTE, LAW, COURSE OF DEALING, CUSTOM AND PRACTICE, OR TRADE USAGE.

DISCLAIMER OF DAMAGES. Anyone using, testing, or evaluating BitDefender bears all risk to the quality and performance of BitDefender. In no event shall SOFTWIN be liable for any damages of any kind, including, without limitation, direct or indirect damages arising out of the use, performance, or delivery of BitDefender, even if SOFTWIN has been advised of the existence or possibility of such damages.

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

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

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

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

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

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

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

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

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

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

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

Preface

This guide is intended to all users who have chosen **BitDefender Mobile Security** as a security solution for their mobile devices. The information presented in this book is accessible to everyone who has a basic knowledge of the mobile device owned and of its operating system.

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

We wish you a pleasant and useful lecture.

1. Conventions Used in This Book

1.1. Typographical Conventions

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

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

1.2. Admonitions

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

Note

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

Important

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

Warning

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

2. The Book Structure

The book consists of 5 parts, containing the major topics: About BitDefender, Product Installation, Description and Features, Configuration and Use, and Getting Help. Moreover, a glossary is provided to clarify some technical terms.

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

Product Installation. Step by step instructions for installing BitDefender on a mobile device. This is a comprehensive tutorial on installing **BitDefender Mobile Security**. Starting with the prerequisites for a successful installation, you are guided through the whole installation process. Finally, the removing procedure is described in case you need to uninstall BitDefender.

Description and Features. **BitDefender Mobile Security**, its components and features are presented to you.

Configuration and Use. Description of basic administration and maintenance of BitDefender. The chapters explain in detail all options of **BitDefender Mobile Security**, how to configure the product and how to use it.

Getting Help. Where to look and where to ask for help if something unexpected appears.

Glossary. The Glossary tries to explain some technical and uncommon terms you will find in the pages of this document.

3. Request for Comments

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

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

Important

Please write all of your documentation-related e-mails in English so that we can process them efficiently.

About BitDefender

1. Who is BitDefender?

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

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

1.1. Why BitDefender?

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

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

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

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

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

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

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

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

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

1.2. About SOFTWIN

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

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

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

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

Product Installation

2. BitDefender Mobile Security - Update Module Installation

The **BitDefender Mobile Security - Update Module Installation** chapter of this user guide contains the following topics:

- System Requirements
- Install
- Repair or Uninstall

2.1. System Requirements

In order for the product to operate properly,, before installing it, make sure that the following system requirements are met:

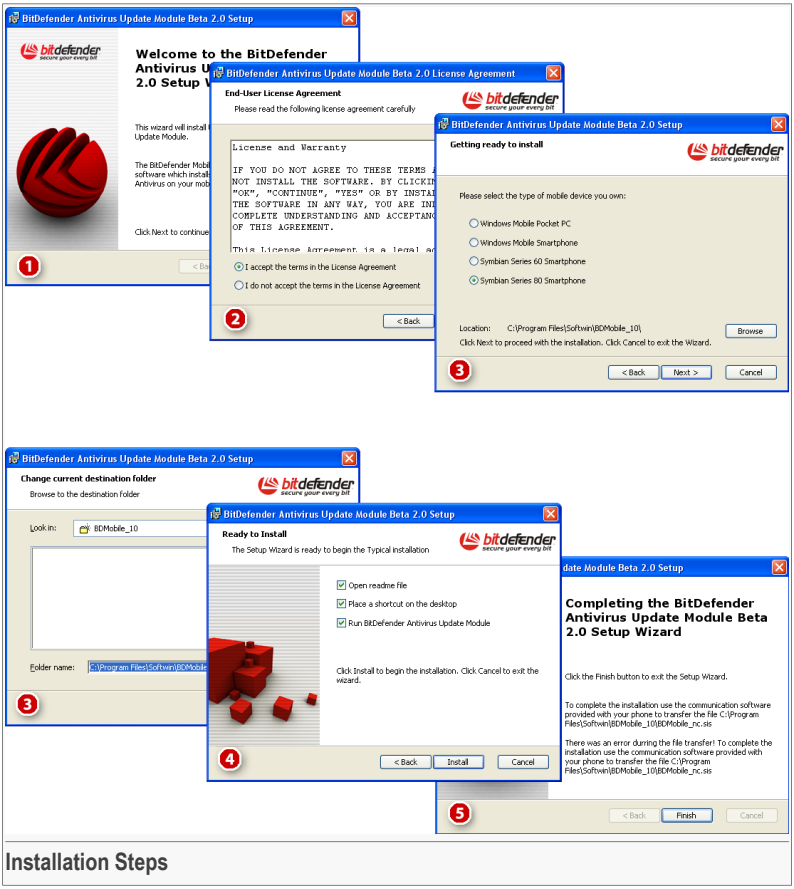
- Pentium MMX 200 MHz or higher processor
- Minimum 64MB of RAM Memory (128MB Recommended)
- Minimum 40MB available hard disk space
- **Operating system** - Windows 2000 (or higher); Internet Explorer 5.0 (or higher)
- **Software** - Microsoft .NET Framework 1.1 (or higher); Microsoft ActiveSync v3.8 (or higher) for Windows Mobile devices; Nokia PC Suite v6.6 (or higher) for Nokia devices with Symbian OS

Important

In order to install **BitDefender Mobile Security** on your device and to update it using the desktop module, you will need an active connection between the device and the PC. Make sure that you can connect the device to the computer (through a cable, infrared or Bluetooth connection).

2.2. Install

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



Installation Steps

1. Click **Next** to continue or click **Cancel** if you want to quit installation.
2. Please read the License Agreement, select **I accept the terms in the License Agreement** and click **Next**. If you do not agree to these terms, click **Cancel**. The installation process will be abandoned and you will exit the setup process.
3. Select the operating system your mobile device works on. These are the available options:
   - **Windows Mobile Pocket PC**
   - **Windows Mobile Smartphone**

- **Symbian Series 60 Smartphone**
- **Symbian Series 80 Smartphone**

You can select the folder where you want to install the product. The default folder is `C:\Program Files\Softwin\BitDefenderMobile2`.

Important

This is where you can find the installation package required to install **BitDefender Mobile Security** on your device. During the installation of the desktop module, the installation package will be automatically sent from this folder to the device. However, if the transfer fails, you will have to send it manually to your device.

If you want to select another folder, click **Browse**. A new window will appear, where you can select the folder you wish BitDefender Mobile Security - Update Module to be installed in. Click **OK** to change the path or **Cancel** to return to the previous window, without making any modifications.

Click **Next** to continue.

4. You have three options selected by default:
   - **Open readme file** - to open the readme file at the end of the installation.
   - **Place a shortcut on the desktop** - to place a shortcut to BitDefender Mobile Security - Update Module on your desktop at the end of the installation.
   - **Run BitDefender Antivirus Desktop Module** - to run BitDefender Mobile Security - Update Module.

Important

Connect the device to the computer in order to install BitDefender Mobile Security on your device.

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

The desktop module will be installed on the computer, along with the installation package for the device running the operating system you chose previously.

Important

During the installation, the BitDefender Mobile Security installation package will be sent to your device. A message will appear informing you whether the file transfer was successful or not.
If the file was successfully sent, you will be asked to continue the installation on your device. Follow the on-screen instructions on your device, as described in the "*BitDefender Mobile Security Installation*" (p. 13) section.
If an error occurred during the file transfer, go to the installation folder and send the installation package to your device, using the appropriate software (Nokia PC Suite

for Symbian devices or Microsoft ActiveSync for Windows Mobile devices). The installation package is:

- `BDMobile.sis` for Symbian devices.
- `BDMobile_nc.sis` for Symbian S80 devices.
- `BD-SmartPhone.cab` for Windows Mobile Smartphone.
- `BD-PocketPC.cab` for Windows Mobile PocketPC.

5. Click **Finish** to complete product installation. If you have accepted the default settings for the installation path, a new folder named `Softwin` will be created in the `Program Files`, with a `BitDefenderMobile2` subfolder.

2.3. Repair or Uninstall

If you want to repair or remove **BitDefender Mobile Security - Update Module**, access the Windows start menu and follow this path: **Start** → **Programs** → **BitDefender** → **Repair or Uninstall**.

You will be requested to confirm your choice by clicking **Next**. A new window will appear and you will be able to select one of the following options:

- **Repair** - to re-install BitDefender Mobile Security - Update Module
- **Remove** - to remove all installed components.

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

3. BitDefender Mobile Security Installation

The **BitDefender Mobile Security Installation** chapter of this user guide contains the following topics:

- Device Requirements
- Install
- Remove

3.1. Device Requirements

In order for the product to operate properly,, before installing it, make sure that the following device requirements are met:

Windows Mobile PocketPC Device Requirements

- **Minimum memory** - 390kB.
- **Operating system** - Windows Mobile Pocket PC v2002 (or higher).
- **Software** - Active Sync.

Windows Mobile Smartphone Device Requirements

- **Minimum memory** - 370kB.
- **Operating system** - Windows Mobile Smartphone v2002 (or higher).
- **Software** - Active Sync.

Symbian S60 Device Requirements

- **Minimum memory** - 200kb.
- **Operating system** - Symbian Os v7; Symbian Os v8.
- **Developer platform** - Series 60 2nd Edition.

Symbian S80 Device Requirements

- **Minimum memory** - 230kb.

- **Operating system** - Symbian Os v7.
- **Developer platform** - Series 80.

Important

In order to install **BitDefender Mobile Security** on your device and to update it using the desktop module, you will need an active connection between the device and the PC. Make sure that you can connect the device to the computer (through a cable, infrared or Bluetooth connection).

3.2. Install

Prerequisites. In order to install **BitDefender Mobile Security** on your mobile device, you need to get the installation package. Please follow these steps:

1. Connect the device to the computer.
2. Install **BitDefender Mobile Security - Update Module** on your computer.

   During the installation of BitDefender Mobile Security - Update Module, the installation package will be automatically sent to your device. If the file transfer has failed, go to the installation folder and send the installation package to your device, using the appropriate software (Nokia PC Suite for Symbian devices or Microsoft ActiveSync for Windows Mobile devices). The installation package is:

   - `BDMobile.sis` for Symbian S60 devices.
   - `BDMobile_nc.sis` for Symbian S80 devices.
   - `BD-SmartPhone.cab` for Windows Mobile Smartphone.
   - `BD-PocketPC.cab` for Windows Mobile PocketPC.

   Note

   For more details check the "*BitDefender Mobile Security - Update Module Installation*" (p. 9) section.

3. You will receive the installation package as a message on your mobile device.

Important

You can also get the installation package directly from the BitDefender website: www.bitdefender.com.

Install on Windows Mobile PocketPC Devices

Note
If you do not install BitDefender Mobile Security using the BitDefender Mobile Security - Update Module, search for the installation package on your device and open it in order to start the installation process.

Follow the on-screen instructions on your device to install BitDefender:

1. Select **Yes** to continue.
2. If you already have BitDefender Mobile Security installed on your device, you will be requested to confirm whether you want to replace the current version or not.

   Note
   If you have an older version of BitDefender, we recommend you to replace it.

   Select **OK** to continue or **Cancel** to cancel installation.
3. Please read the End User License Agreement. If you do not agree to these terms, remove BitDefender from your device (see "Remove from Windows Mobile PocketPC Devices" (p. 18)).

Install on Windows Mobile Smartphone Devices

Note
If you do not install BitDefender Mobile Security using the BitDefender Mobile Security - Update Module, search for the installation package on your device and open it in order to start the installation process.

Follow the on-screen instructions on your device to install BitDefender:

1. Select **Yes** to continue.
2. If you already have BitDefender Mobile Security installed on your device, you will be requested to confirm whether you want to replace the current version or not.

   Note
   If you have an older version of BitDefender, we recommend you to replace it.

   Select **OK** to continue or **Cancel** to cancel installation.
3. Choose where to install BitDefender Mobile Security. Two options are available:

- **Phone** - to install BitDefender in the phone memory.
- **/Storage Card** - to install BitDefender on the storage card.

You can see the minimum space required by the application and the space available on the media.

Select **Done**.

Note

If you have chosen to replace a previously installed version, you will be requested to restart the device at the end of the installation. Select **OK**.

4. Please read the End User License Agreement. If you do not agree to these terms, remove BitDefender from your device (see "Remove from Windows Mobile Smartphone Devices" (p. 18)).

Install on Symbian S60 Devices

Note

If you do not install BitDefender Mobile Security using the BitDefender Mobile Security - Update Module, use a file browser to locate the installation package and open it in order to start the installation process.

Follow the on-screen instructions on your device to install BitDefender:

1. Select **Yes** to continue.
2. A message requesting you to confirm the installation will appear.

   Select **Yes** to install BitDefender. If you choose **No**, the installation process will be cancelled.
3. If you already have BitDefender Mobile Security installed on your device, you will be requested to confirm whether you want to replace the current version or not.

   Note

   If you have an older version of BitDefender, we recommend you to replace it.

   Select **Yes** to continue or **No** to cancel installation.
4. If you have confirmed the installation process, a menu containing the following options will appear:
   - **Install** - to install **BitDefender Mobile Security** on your device.
   - **View certificate** - to view the BitDefender certificate.

- **View details** - to view information about **BitDefender Mobile Security**.

Select **Install** to start the installation process.

5. Please read the End User License Agreement and select **OK** to finish installation. If you do not agree to these terms, select **Cancel** to cancel installation.
6. If the installation was completed successfully, a confirmation message will appear. Now, your device is protected by **BitDefender Mobile Security**.

Install on Symbian S80 Devices

Note

If you do not install BitDefender Mobile Security using the BitDefender Mobile Security - Update Module, use a file browser to locate the installation package and open it in order to start the installation process.

Follow the on-screen instructions on your device to install BitDefender:

1. Select **Install Anyway** to continue.
2. A message requesting you to confirm the installation will appear.

   If you want to view information about **BitDefender Mobile Security**, select **Details**.

   Select **Install** to install BitDefender. If you choose **Cancel**, the installation process will be cancelled.
3. If you already have BitDefender Mobile Security installed on your device, you will be requested to confirm whether you want to replace the current version or not.

   Note

   If you have an older version of BitDefender, we recommend you to replace it.

   Select **Replace** to continue or **Cancel** to cancel installation.
4. Please read the End User License Agreement and select **OK** to finish installation. If you do not agree to these terms, select **Cancel** to cancel installation.
5. You can choose where to place a BitDefender shortcut. Use the **Select** command to create a BitDefender shortcut in a group. If you want to create a new group, select **New group**.

   Select **OK** to continue.
6. If the installation was completed successfully, a confirmation message will appear. Select **OK**. Now, your device is protected by **BitDefender Mobile Security**.

3.3. Remove

Remove from Windows Mobile PocketPC Devices

If you want to remove **BitDefender Mobile Security** from your Windows Mobile PocketPC device, you must follow these steps:

1. Tap **Start** → **Settings** → **System** → **Remove Programs**.
2. Locate **BitDefender** in the list and tap it.
3. Tap **Remove**.
4. You will be asked to confirm your choice. Tap **Yes** to remove BitDefender Mobile Security from your device.

Remove from Windows Mobile Smartphone Devices

If you want to remove **BitDefender Mobile Security** from your Windows Mobile Smartphone device, you must follow these steps:

1. Select **Start** → **Settings** → **Remove Programs**.
2. Locate **BitDefender** in the list.
3. From the menu, select **Remove**.
4. You will be asked to confirm your choice. Select **Yes** to remove BitDefender Mobile Security from your device.

Remove from Symbian S60 Devices

If you want to remove **BitDefender Mobile Security** from your Symbian S60 device, you must follow these steps:

1. From the phone menu, select **Tools** → **Manager** to enter the **Application manager**.
2. Locate **BitDefender** in the list.
3. From the **Options** menu, select **Remove**.
4. You will be asked to confirm your choice. Select **Yes** to remove BitDefender Mobile Security from your device.

Remove from Symbian S80 Devices

If you want to remove **BitDefender Mobile Security** from your Symbian S80 device, you must follow these steps:

1. Select **Tools** → **Control Panel** → **Data Management** → **Application manager** from the phone menu to enter the **Application manager**.
2. Locate **BitDefender** in the list.
3. Select **Remove**.
4. You will be asked to confirm your choice. Select **OK** to remove BitDefender Mobile Security from your device.

Description and Features

4. BitDefender Mobile Security

BitDefender Mobile Security provides permanent antivirus protection for mobile devices running SymbianTM or Microsoft® Windows Mobile™. Relying on the valuable BitDefender experience in fighting computer threats, **BitDefender Mobile Security** is a light, easy to use instrument that will keep your mobile device on the move.

4.1. Features

BitDefender Mobile Security comes to solve the basic protection needs of your mobile device. The following features make **BitDefender Mobile Security** the best choice for protecting your mobile device:

Permanent antivirus protection. The virus shield runs at start up and continuously monitors the device, preventing the execution of infected files.

On-demand virus scan. Using the award-wining BitDefender technologies, the product can check the internal memory, memory card or the entire device, removing the malicious files found. The scanning engines are also capable of detecting infected files within common archive types.

Fast, flexible updates. The product can be updated either via GPRS from the service provider or from an internet-connected PC. The virus definitions updates are provided by the BitDefender Lab, an industry leader in terms of response time to virus outbreaks.

Engineered for mobility. Optimized scanning processes provide permanent protection while minimizing resource consumption for a longer battery life.

Easy to install and to use. The product can be installed directly to the mobile device, via a mobile Internet connection or via the PC application. The interface is simple and friendly and no user intervention is required while the product is running.

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

Configuration and Use

5. Windows Mobile Pocket PC Devices

The **Windows Mobile Pocket PC Devices** chapter of this user guide contains the following topics:

- Overview
- Scan
- Report
- Shield
- Update
- Register

5.1. Overview

BitDefender Mobile Security is the application installed on your mobile device so as to protect it against viruses and other malware.

5.1.1. Getting Started

To start BitDefender, tap **Start** → **Programs**, then browse for the **BitDefender icon** and tap it. If you are using a registered version, the main screen will be displayed.

If you are using a trial version, each time you open **BitDefender Mobile Security**, you will be requested to register the product.

Trial Version

Important

This also happens if the product has expired or is about to expire (the last 3 days of the licensing period).

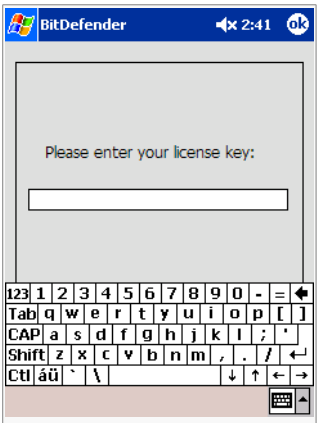
Tap **Register** to register the product or **OK** to continue evaluating the product.

If you tap **Register**, a dialog asking you to enter the license key will appear.

Enter a valid license key and tap **OK** to use the registered version.

Important

The license key is a 20-character alphanumerical string!



Register Trial Version

If you tap **OK**, the main screen will be displayed. If you decide to register the product later during the session, you can do that in the Register section.

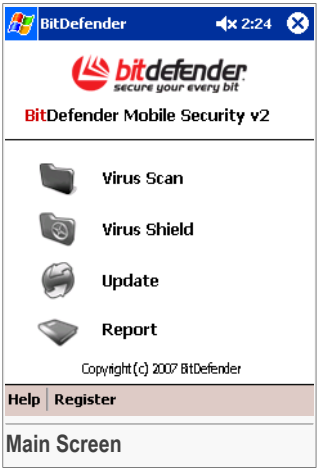
5.1.2. Main Screen

This is where you get access to all BitDefender sections.

The following options are available:

- **Scan** - to access the **Scan** section.
- **Shield** - to access the **Shield** section.
- **Update** - to access the **Update** section.
- **Report** - to access the **Report** section.

To open a section, tap the corresponding icon.



Main Screen

Note

To find more information about each section, check the corresponding section in this chapter.

On the left bottom side of the display, two options are available:

- **Register** - to access the **Register** section.
- **Help** - to access the help file.

  A contextual help is accessible in each section (by tapping **Help**) for a better understanding of the topics related to the respective section.

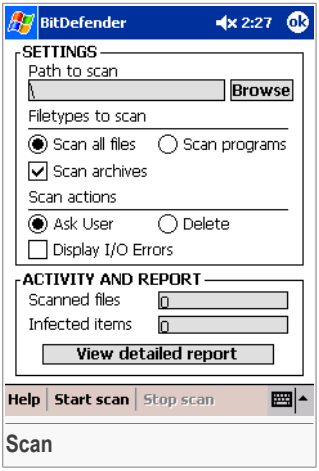
Tap **X** in the top right corner of the display to exit BitDefender.

5.2. Scan

To access this section choose **Scan** from the main screen.

This is where you can configure the scan settings, scan your device and see the scan results.

Tap **OK** to return to the main screen.



5.2.1. Configuring the Scan Options

Important

By default, BitDefender will scan all your files, except for archives, and prompt you for action.

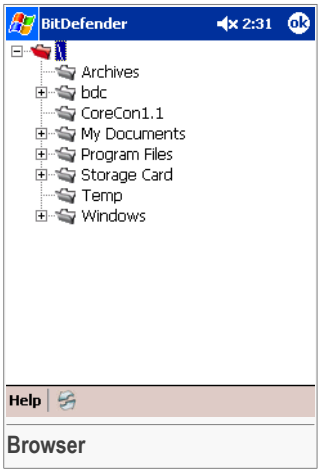
In the Scan section you can see a list of options that allow you to configure the scan settings. The following options are available:

- **Scan path** - to specify the scan target. In the edit box, provide the path to the files or folders you want to be scanned.

  An easier method to specify the scan target is to use the browser:

  1. Tap **Browse** on the right side of the edit box to open the browser. A new screen, containing the folder list, will appear.
  2. Browse through the folder list to find the scan target. To expand / collapse objects tap the + / – signs corresponding to the respective objects.

     To return to the default path, tap the **Refresh icon** from the left bottom side of the display.
  3. Select **OK** to set the scan target. The new path will appear in the **Scan path** field.

  Note

  The default path is: \. With this option, all your files will be scanned.

- **Scan files** - to specify the type of files to be scanned.

  Two options are available:

Option	Description
All files	All files will be scanned for viruses and other malware.
Only programs	Only program files will be scanned for viruses and other malware. This means that only the files with an `.exe`, `.app` and `.dll` extension will be scanned.

  Tap the desired option in order to select it.

  Note

  By default, all files will be scanned.

- **Scan archives** - check this option to scan inside archives.

Note

By default, archives will not be scanned.

- **Scan action** - to specify the action mode.

  Two options are available:

Option	Description
Ask user	When an infected file is found, BitDefender will prompt the user for action. You must confirm your choice by selecting **Delete / Ignore**. If several files are detected as infected, you can apply the action to all infected files by tapping **Apply to all infected**.
Delete	Infected files will be automatically deleted.

  Tap the desired option in order to select it.

Note

By default, the user will be prompted for action.

- **Display I/O Errors** - check this option to log the I/O errors in the report file.

Note

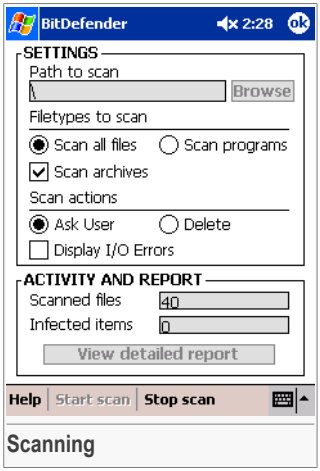
By default, the I/O errors will not be logged in the report file.

5.2.2. Scanning the Device

To initiate the scanning process, tap **Start scan** at the bottom of the screen.

If an infected file is detected, depending on the scan action selected, it will be automatically deleted or you will be prompted for action.

The scanning process can be cancelled at any moment by tapping **Stop scan** at the bottom of the screen.



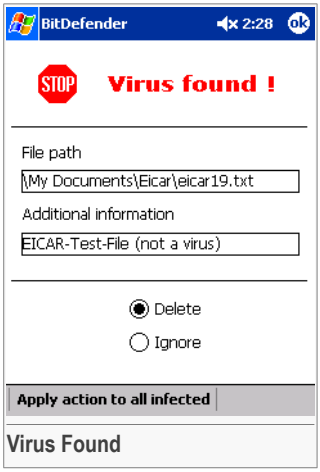
Scanning

Note

This option is enabled only during scanning!

If the **Ask user** option is enabled, you will be prompted for action everytime an infected file is detected. A new screen will appear, providing you with information about the detected virus.

Choose **Delete** to delete the file or **Ignore** to ignore the infection.



Virus Found

Warning

If you choose **Ignore**, your system will not be protected.

Tap **Apply to all infected** if you want to apply the action to all infected files.

Select **OK** to apply the action and resume scanning.

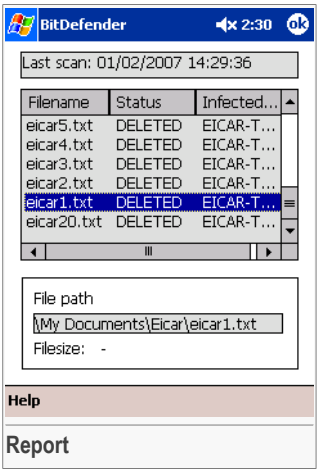
At the end of the scanning process, you will be directed to the Report section where you can view the scan results.

5.3. Report

To access this section choose **Report** from the main menu. You can also access it from the **Scan** section (tap **Report**).

Note

At the end of each scanning process, you will be directed to this section to view the scan results.



This is where you can see the list of all of the infected files detected during the last successful scan. The path, the name of the virus and its viral status are provided for each file.

The date and time of the last scan are given at the top of the screen.

Select **OK** to return to the previous screen.

5.3.1. Viewing the Scan Results

The report file consists of a list of all of the infected files. It can also contain I/O errors, if you have selected the **Display I/O Errors** option from the **Scan** section.

Note

Most of the I/O errors occur while scanning ROM files. They are not necessarily security breaches.

If you tap an item from the list, you can see more information about the respective file

There are two types of logged files: infected files and I/O errors. For an infected file, the following are provided: virus name, disinfection status (**Deleted** / **Deletion failed**), path and, possibly, file size. For an I/O error, the following are provided: status (**I/O Error**), path and file size.

5.4. Shield

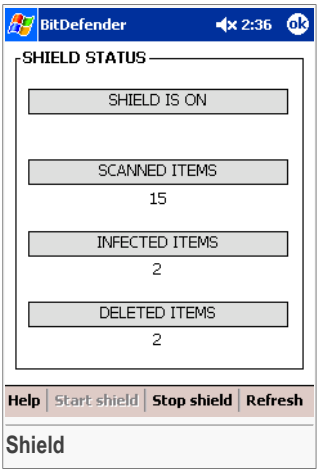
To access this section choose **Shield** from the main screen.

This is where you can enable / disable real-time protection and view the shield statistics.

You can see the number of scanned / infected / disinfected files per session. A session starts when you turn the shield on and it ends when you turn the shield off.

To update the shield statistics, tap **Refresh**.

Tap **OK** to return to the main screen.



Shield

5.4.1. Configuring the Shield

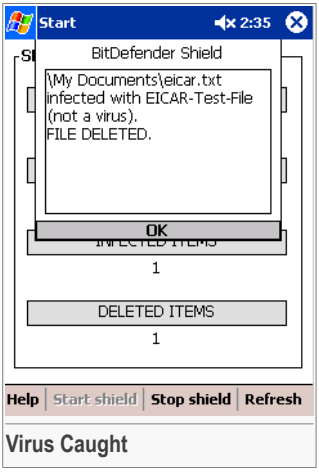
To turn real-time protection on / off, tap **Start shield** / **Stop shield**.

Warning

Keep the shield on to protect your device from malware!

If enabled, the shield will permanently monitor your device, preventing the execution of infected files. When an infected file is detected, an alert will appear informing you about the infection.

Select **OK** to close the alert message.



Virus Caught

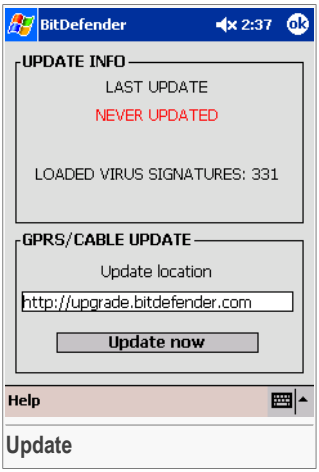
5.5. Update

To access this section choose **Update** from the main menu.

This is where you can initiate the update via the device and view update information (the date and time of the last successful update and the update status).

Select **OK** to return to the main screen.

Tap **Help** to access the contextual help file.



5.5.1. Setting the Update Address

To change the url address of the update server you have to enter a new update location in the edit box.

Note

The default location is `http://upgrade.bitdefender.com`.

5.5.2. Updating BitDefender

There are two ways of updating BitDefender:

- Update via Device
- Update via PC

Update via Device

BitDefender can be updated anytime you want by connecting to the Internet directly from the device. The process consists of downloading the update file on the mobile device from the update server and reinstalling the application on the device.

Important

To connect via GPRS, make sure the GPRS service is activated and the appropriate settings are installed on your device. If not, contact your mobile phone operator in order to activate GPRS and to receive the GPRS settings.

Follow these steps to update BitDefender via the device:

1. Connect the device to the PC if you want to use the Internet connection of your computer.

   Note

   If you do not connect the device to the PC and you do not have a wireless Internet connection either, BitDefender will connect to the update server via GPRS, if available.

2. Set the address of the update server. For more information, check the "*Setting the Update Address*" (p. 35) section.

   Note

   This step is optional!

3. Tap **Update**.

   BitDefender will connect to the update server and download the update file on the device.

4. Once the update file has been transferred on your device, BitDefender will be closed and the installer will start. Follow the on-screen instructions on your device to reinstall the updated application.

   Note

   For detailed information about the installation steps on your device, check "*Install*" (p. 14).

5. If the update was successful, a message will appear. Select **OK** to restart the application.

Update via PC

BitDefender can be updated using the desktop application. The process consists of downloading the update file on an Internet-connected computer, transferring it to the mobile device and reinstalling the application on the device.

Important

Microsoft ActiveSync must be installed on your computer in order to update BitDefender Mobile Security via PC.

Follow these steps to update BitDefender via PC:

1. Connect the device to the PC (through Bluetooth™, infrared or cable).
2. Download the update file to the PC using the desktop application (in the Update section, click **Update now**).

   The desktop module will connect to the device, download the update file on your computer and transfer it on your device

   Note

   If the device is not connected to the PC or if the product is not valid, the update process will be cancelled.

3. Once the update file has been transferred on your device, BitDefender will be closed and the installer will start. Follow the on-screen instructions on your device to reinstall the updated application.

   Note

   For detailed information about the installation steps on your device, check "*Install*" (p. 14).

4. If the update was successful, a message will appear. Select **OK** to restart the application.

Note

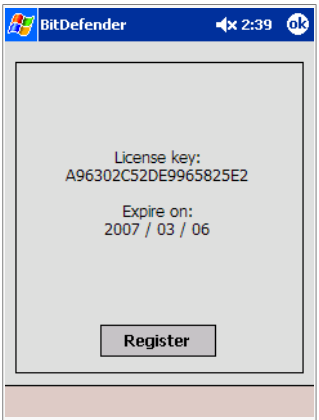
For more information about the desktop application, check the BitDefender Mobile Security - Update Module chapter of this user guide.

5.6. Register

To access this section choose **Register** from the main screen.

This is where you can register the product and see the current BitDefender license key and its expiration date.

Tap **OK** to return to the main screen.



Register

5.6.1. Registering BitDefender Mobile Security

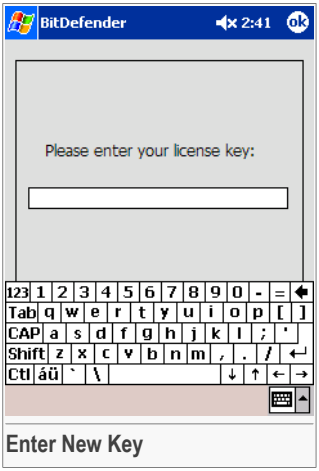
To register the product or change the license key tap **New key**. A dialog will appear.

Enter a valid license key and select **OK**.

Important

The license key is a 20-character alphanumerical string!

If you want to return to the **Register** section without changing the license key, select **OK**.



Enter New Key

6. Windows Mobile Smartphone Devices

The **Windows Mobile Smartphone Devices** chapter of this user guide contains the following topics:

- Overview
- Scan
- Report
- Shield
- Update
- Register

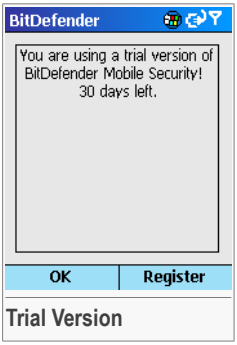
6.1. Overview

BitDefender Mobile Security is the application installed on your mobile device so as to protect it against viruses and other malware.

6.1.1. Getting Started

To start BitDefender, browse for the **BitDefender icon** in the Start menu and then press the action button. If you are using a registered version, the main screen will be displayed.

If you are using a trial version, each time you open **BitDefender Mobile Security**, you will be requested to register the product.



Important

This also happens if the product has expired or is about to expire (the last 3 days of the licensing period).

You can choose:

- **Register** - to register the product.
- **Continue** - to continue evaluating the product.

If you choose **Register**, a dialog will appear.

Enter a valid license key and select **OK** to use the registered version.

Important

The license key is a 20-character alphanumerical string!

Select **Back** to continue evaluating the product.

Register Trial Version

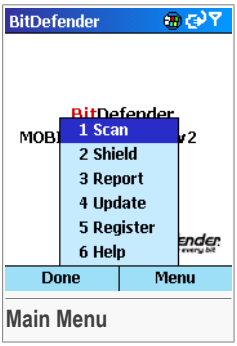
If you choose **Continue**, the main screen will be displayed. If you decide to register the product later during the session, you can do that in the Register section.

6.1.2. Main Screen

This is where you get access to all BitDefender sections.

Main Screen

If you select **Menu**, the main menu of the application will appear. On the menu, the following commands are available:



- **Scan** - to access the **Scan** section.
- **Shield** - to access the **Shield** section.
- **Report** - to access the **Report** section.
- **Update** - to access the **Update** section.
- **Register** - to access the **Register** section.
- **Help** - to access the help file.

  A contextual help file is accessible in each section (by selecting **Help** from the **Menu**) for a better understanding of the topics related to the respective section.

Note

To find more information about each section, check the corresponding section in this chapter.

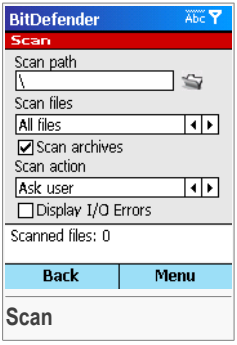
To exit BitDefender select **Done**.

6.2. Scan

To access this section choose **Scan** from the main menu.

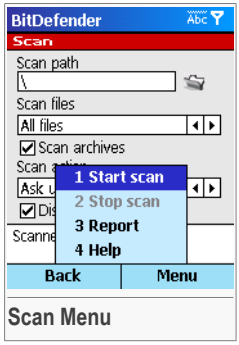
This is where you can configure the scan settings, scan your device and see the scan results.

Select **Menu** to open the contextual menu or **Back** to return to the main screen.



6.2.1. Scan Menu

If you select **Menu**, a contextual menu will appear. The following commands are available:



Scan Menu

- **Start scan** - to initiate a scan process.
- **Stop scan** - to stop the current scan process.

Note
This option is enabled only during scanning!

- **Report** - to access the Report section, where you can see the report file of the last successful scan.
- **Help** - to access the contextual help file.

6.2.2. Configuring the Scan Options

Important
By default, BitDefender will scan all your files, except for archives, and prompt you for action.

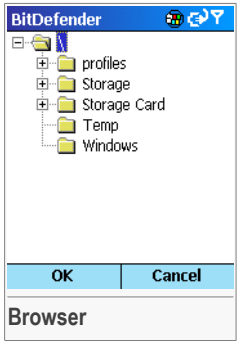
In the Scan section you can see a list of options that allow you to configure the scan settings. The following options are available:

- **Scan path** - to specify the scan target. In the edit box, provide the path to the files or folders you want to be scanned.

  An easier method to specify the scan target is to use the browser:

  1. Select the **Browse icon** from the right side of the edit box and press the action button to open the browser. A new screen, containing the folder list, will appear.
  2. Use the navigation button to browse through folders and find the scan target. To expand / collapse objects press the action button.
  3. Select **OK** to set the scan target. The new path will appear in the **Scan path** field.

     To return to the previous screen without making any changes select **Cancel**.



Browser

Note

The default path is: \. With this option, all your files will be scanned.

- **Scan files** - to specify the type of files to be scanned.

  Two options are available:

Option	Description
All files	All files will be scanned for viruses and other malware.
Only programs	Only program files will be scanned for viruses and other malware. This means that only the files with an `.exe`, `.app` and `.dll` extension will be scanned.

  Use the navigation button to choose the desired option.

Note

By default, all files will be scanned.

- **Scan archives** - check this option to scan inside archives.

Note

By default, archives will not be scanned.

- **Scan action** - to specify the action mode.

  Two options are available:

Option	Description
Ask user	When an infected file is found, BitDefender will prompt the user for action. You must confirm your choice by selecting **Delete / Ignore**. If several files are detected as infected, you can apply the action to all infected files by checking the **Apply to all infected** option.
Delete	Infected files will be automatically deleted.

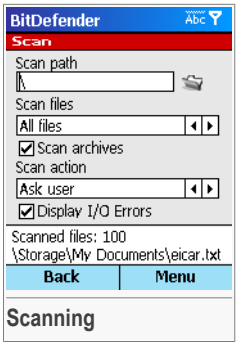
  Use the navigation button to choose the desired option.

Note
By default, the user will be prompted for action.

- **Display I/O Errors** - check this option to log the I/O errors in the report file.

Note
By default, the I/O errors will not be logged in the report file.

6.2.3. Scanning the Device

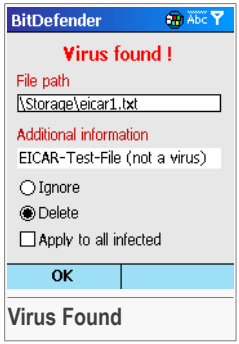


To initiate the scanning process, select **Start scan** from the Scan menu.

You can see the last file scanned. If an infected file is detected, depending on the scan action selected, it will be automatically deleted or you will be prompted for action.

The scanning process can be cancelled at any moment by selecting **Stop scan** from the contextual menu.

If the **Ask user** option is enabled, you will be prompted for action everytime an infected file is detected. A new screen will appear, providing you with information about the detected virus.



Choose **Delete** to delete the file or **Ignore** to ignore the infection.

Warning
If you choose **Ignore**, your system will not be protected.

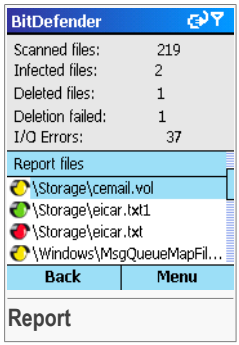
Check **Apply to all infected** if you want to apply the action to all infected files.

Select **OK** to apply the action and resume scanning.

At the end of the scanning process, you will be directed to the Report section where you can view the scan results.

6.3. Report

To access this section choose **Report** from the main menu. You can also access it from the **Scan** section (choose **Report** from the Scan menu).



Note

At the end of each scanning process, you will be directed to this section to view the scan results.

This is where you can see the scan statistics and the list of all of the infected files detected during the last successful scan. The path, the name of the virus and the disinfection status are provided for each file.

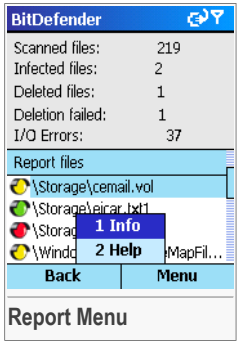
You can see the number of scanned / infected / deleted files and the number of I/O errors as well as of deletion failures for the last scan event.

Select **Menu** to open the contextual menu or **Back** to return to the previous screen.

6.3.1. Report Menu

If you select **Menu**, a contextual menu will appear. The following commands are available:

- **Info** - to see all information about a selected infected file.
- **Help** - to access the contextual help file.



6.3.2. Viewing the Scan Results

The report file consists of a list of all of the infected files. It can also contain I/O errors, if you have selected the **Display I/O Errors** option from the Scan section.

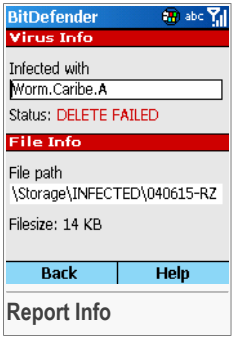
Note

Most of the I/O errors occur while scanning ROM files. They are not necessarily security breaches.

An icon indicates the status of each item in the report file, as presented further:

- - the infected file was deleted.
- - the infected file was not deleted.
- - this is an I/O error.

To see all information about an item, select the item from the list and choose **Info** from the Report menu. By selecting this option, a new screen will appear.



There are two types of logged files: infected files and I/O errors. For an infected file, the following are provided: virus name, disinfection status (**Deleted** / **Deletion failed**), path and, possibly, file size. For an I/O error, the following are provided: status (**I/O Error**), path and file size.

Select **Back** to return to the Report section.

6.4. Shield

To access this section choose **Shield** from the main menu.

This is where you can enable / disable real-time protection and view the shield statistics.

You can see the number of scanned / infected / disinfected files per session. A session starts when you turn on the shield and it ends when you turn the shield off.

Select **Menu** to open the contextual menu or **Back** to return to the main screen.

6.4.1. Shield Menu

If you select **Menu**, a contextual menu will appear. The following commands are available:

- **Start shield** - to turn real-time protection on.
- **Stop shield** - to turn real-time protection off.
- **Refresh** - to refresh the shield statistics.
- **Help** - to access the contextual help file.

Note

Only one of the first two commands is enabled at a time.

Shield Menu

6.4.2. Configuring the Shield

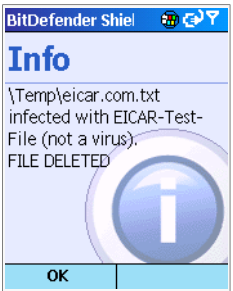
To turn real-time protection on / off, select **Start shield** / **Stop shield** from the contextual menu.

Warning

Keep the shield on to protect your device from malware!

If enabled, the shield will permanently monitor your device, preventing the execution of infected files. When an infected file is detected, an alert will appear informing you about the infection.

Select **OK** to close the alert message.



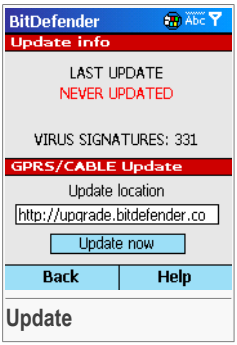
Virus Caught

6.5. Update

To access this section choose **Update** from the main menu.

This is where you can initiate the update via the device and view update information (the date and time of the last successful update and the update status).

Select **Help** to access the help file or **Back** to return to the main screen.



6.5.1. Setting the Update Address

To change the url address of the update server you have to enter a new update location in the edit box.

Note

The default location is `http://upgrade.bitdefender.com`.

6.5.2. Updating BitDefender

There are two ways of updating BitDefender:

- Update via Device
- Update via PC

Update via Device

BitDefender can be updated anytime you want by connecting to the Internet directly from the device. The process consists of downloading the update file on the mobile device from the update server and reinstalling the application on the device.

Important

To connect via GPRS, make sure the GPRS service is activated and the appropriate settings are installed on your device. If not, contact your mobile phone operator in order to activate GPRS and to receive the GPRS settings.

Follow these steps to update BitDefender via the device:

1. Connect the device to the PC if you want to use the Internet connection of your computer.

   Note
   If you do not connect the device to the PC and you do not have a wireless Internet connection either, BitDefender will connect to the update server via GPRS, if available.

2. Set the address of the update server. For more information, check "*Setting the Update Address*" (p. 48).

   Note
   This step is optional!

3. Select **Update**.

   BitDefender will connect to the update server and download the update file on the device.

4. Once the update file has been transferred on your device, BitDefender will be closed and the installer will start. Follow the on-screen instructions on your device to reinstall the updated application.

   Note
   For detailed information about the installation steps on your device, check "*Install*" (p. 14).

5. If the update was successful, a message will appear. Select **OK** to restart the application.

Update via PC

BitDefender can be updated using the desktop application. The process consists of downloading the update file on an Internet-connected computer, transferring it to the mobile device and reinstalling the application on the device.

Important
Microsoft ActiveSync must be installed on your computer in order to update BitDefender Mobile Security via PC.

Follow these steps to update BitDefender via PC:

1. Connect the device to the PC (through Bluetooth™, infrared or cable).
2. Download the update file to the PC using the desktop application (in the Update section, click **Update now**).

   The desktop module will connect to the device, download the update file on your computer and transfer it on your device

   Note
   If the device is not connected to the PC or if the product is not valid, the update process will be cancelled.

3. Once the update file has been transferred on your device, BitDefender will be closed and the installer will start. Follow the on-screen instructions on your device to reinstall the updated application.

   Note
   For detailed information about the installation steps on your device, check "*Install*" (p. 14).

4. If the update was successful, a message will appear. Select **OK** to restart the application.

Note
For more information about the desktop application, check the BitDefender Mobile Security - Update Module chapter of this user guide.

6.6. Register

To access this section choose **Register** from the main menu.

This is where you can register the product and see the current BitDefender license key and its expiration date.

Select **Menu** to open the contextual menu or **Back** to return to the previous screen.

6.6.1. Register Menu

If you select **Menu**, a contextual menu will appear. The following commands are available:

- **New key** - to register the product.
- **Help** - to access the contextual help file.

Register Menu

6.6.2. Registering BitDefender Mobile Security

To register the product or change the license key select **Register** from the menu. A new screen will appear.

Enter a valid license key and select **OK**.

Important

The license key is a 20-character alphanumerical string!

If you want to return to the **Register** section without changing the license key, select **Back**.

Enter New Key

7. Symbian S60 Devices

The **Symbian S60 Devices** chapter of this user guide contains the following topics:

- Overview
- Scan
- Report
- Shield
- Update
- Register

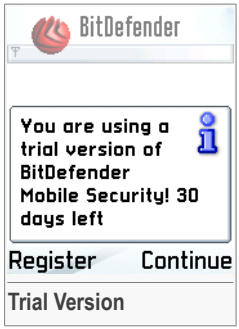
7.1. Overview

BitDefender Mobile Security is the application installed on your mobile device so as to protect it against viruses and other malware.

7.1.1. Getting Started

To start BitDefender, browse for the **BitDefender icon** in the phone menu and then either press the action button or select **Open** from the **Options** menu. If you are using a registered version, the main screen will be displayed.

If you are using a trial version, each time you open **BitDefender Mobile Security**, you will be requested to register the product.



Important

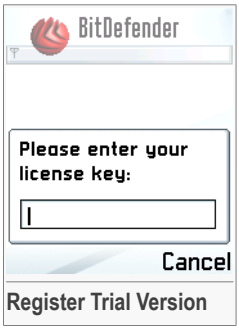
This also happens if the product has expired or is about to expire (the last 3 days of the licensing period).

You can choose:

- **Register** - to register the product.
- **Continue** - to continue evaluating the product.

If you choose **Register**, a dialog asking you to enter the license key will appear.

Enter a valid license key and select **OK** to use the registered version.



Important
The license key is a 20-character alphanumerical string!

Select **Cancel** to continue evaluating the product.

If you choose **Continue**, the main screen will be displayed. If you decide to register the product later during the session, you can do that in the Register section.

7.1.2. Main Screen

This is where you get access to all BitDefender sections.

If you select **Menu**, the main menu of the application will appear. On the menu, the following commands are available:

- **Scan** - to access the **Scan** section.
- **Shield** - to access the **Shield** section.
- **Report** - to access the **Report** section.
- **Update** - to access the **Update** section.
- **Register** - to access the **Register** section.
- **Help** - to access the help file.

A contextual help file is accessible in each section (by selecting **Help** from the **Options** menu) for a better understanding of the topics related to the respective section.

- **Exit** - to exit the application. You can also exit the application by selecting **Exit** from the right bottom side of the main screen.

Note

To find more information about each section, check the corresponding section in this chapter.

7.2. Scan

To access this section choose **Scan** from the main menu.

This is where you can configure **BitDefender Mobile Security** to scan your device.

Select **Options** to open the contextual menu or **Back** to return to the main screen.

7.2.1. Scan Menu

If you select **Options**, a contextual menu will appear. The following commands are available:

- **Start scan** - to initiate a scan process.
- **Select path** - to set the scan target using the browser.
- **Help** - to access the contextual help file.
- **Exit** - to exit the application.

7.2.2. Configuring the Scan Options

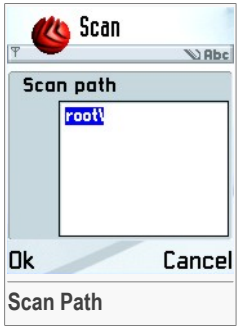
Important

By default, BitDefender will scan all your files, except for archives, and prompt you for action.

In the Scan section you can see a list of options that allow you to configure the scan settings. The following options are available:

- **Scan path** - to specify the scan target. By selecting this option, an edit box will appear.

  Provide the path to the files or folders you want to be scanned and select **OK**. If you want to return to the previous screen without making any changes, select **Cancel**.

  Important

  Every path you type must end in a **backslash "\"** to be valid. Otherwise, when you start a scan process an error message will appear and the scan will be cancelled.

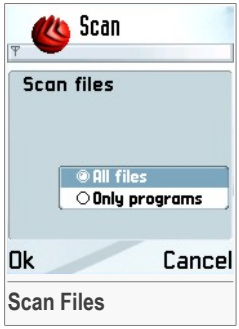
  Note

  The default path is: `root\`. With this option, all your files will be scanned.

  An easier method to specify the scan target is to use the browser. For more information, please check "*Setting the Scan Target Using the Browser*" (p. 58).

- **Scan files** - to specify the type of files to be scanned. By selecting this option, a new screen will appear.

  Two options are available:

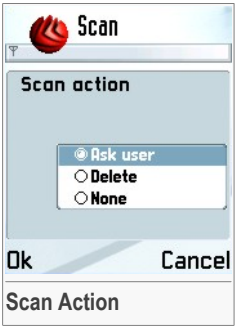
Option	Description
All files	All files will be scanned for viruses and other malware.
Only programs	Only program files will be scanned for viruses and other malware. This means that only the files with an `.exe`, `.app` and `.dll` extension will be scanned.

Choose the desired option and select **OK**. If you want to return to the previous screen without making any changes, select **Cancel**.

Note
By default, all files will be scanned.

- **Scan action** - to specify the action mode. By selecting this option, a new screen will appear.

Note
By default, the user will be prompted for action.



Three options are available:

Option	Description
Ask user	When an infected file is found, BitDefender will prompt the user for action. You must confirm your choice by selecting **Yes / No**. If several files are detected as infected, there is the possibility to apply the last action taken to all infected files. When the virus alert having the **Apply to all?** status appears, choose **Yes** or **No**, depending on whether you want to apply the last action taken to all infected files or not.
Delete	Infected files will be automatically deleted.
None	Infected files will be ignored.

Choose the desired option and select **OK**. If you want to return to the previous screen without making any changes, select **Cancel**.

- **Scan archives** - to specify whether to scan inside archives or not. By selecting this option, a new screen will appear.

Two options are available:

Option	Description
No	Archives will not be scanned.
Yes	Archives will be scanned.

Choose the desired option and select **OK**. If you want to return to the previous screen without making any changes, select **Cancel**.

Note

By default, archives will not be scanned.

7.2.3. Setting the Scan Target Using the Browser

The scan target can be set using the **Scan Path** option. However, if you do not know the precise path to the file or folder you want to scan, you will not be able to use this option. In order to help you choose the scan target easier, **BitDefender Mobile Security** comes with a browser.

To use the browser, choose **Select path** from the Scan menu. A new screen will appear.

The list of all available memory types is displayed: Flash, RAM, ROM and MMC. Using the navigation button, you can browse through the list to find the desired scan target.

Important

Only folders are listed!

Select **Back** to return to the previous screen without making any changes.

If you select **Options**, a contextual menu will be displayed. The following commands are available:

- **Select path** - to choose the selected folder as scan target.
- **Scan all drives** - to choose all the drives to be scanned.
- **Help** - to access the contextual help file.
- **Exit** - to exit the application.

If you choose **Select path** or **Scan all drives**, you will return to the Scan section and the new path will appear in the **Scan path** section.

Select Path Menu

7.2.4. Scanning the Device

To initiate the scanning process, select **Start scan** from the Scan menu. A new screen will appear where you can see details about the files that are being scanned.

Scanning

You can see the last file scanned. If an infected file is detected, depending on the scan action selected, it will be automatically deleted, ignored or you will be prompted for action.

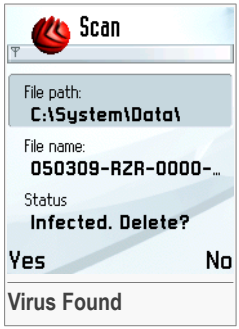
The scanning process can be cancelled at any moment by selecting **Stop**.

If the **Ask user** option is enabled, you will be prompted for action everytime an infected file is detected. A new screen will appear, providing you with information about the detected virus.

Choose **Yes** to delete the file or **No** to ignore the infection.

Warning

If you choose **No**, your system will not be protected.



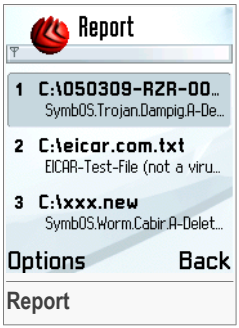
Virus Found

If several files are detected as infected, there is the possibility to apply the last action taken to all infected files. When the virus alert having the **Apply to all?** status appears, choose **Yes** or **No**, depending on whether you want to apply the last action taken to all infected files or not.

At the end of the scanning process, you will be directed to the Report section where you can view the scan results.

7.3. Report

To access this section choose **Report** from the main menu.



Note

At the end of each scanning process, you will be directed to this section to view the scan results.

This is where you can see the list of all of the infected files detected during the last successful scan. The path, the name of the virus and the disinfection status are provided for each file.

Select **Options** to open the contextual menu or **Back** to return to the previous screen.

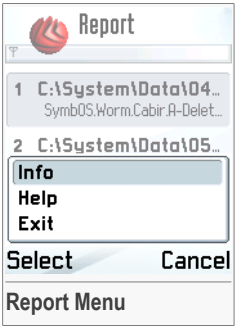
Note

If no virus was detected the message *No virus found* will appear instead.

7.3.1. Report Menu

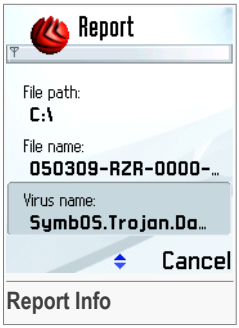
If you select **Options**, a contextual menu will appear. The following commands are available:

- **Info** - to see all information about a selected infected file.
- **Help** - to access the contextual help file.
- **Exit** - to exit the application.



7.3.2. Viewing the Scan Results

To see all information about an infected file, select the file from the list and choose **Info** from the **Report menu**. By selecting this option, a new screen will appear.



You can see the filename and its path, the name of the virus and the disinfection status.

Select **Cancel** to return to the Report section.

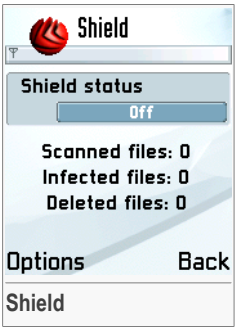
7.4. Shield

To access this section choose **Shield** from the main menu.

This is where you can enable / disable real-time protection and view the shield statistics.

You can see the number of scanned / infected / disinfected files per session. A session starts when you turn on the shield and it ends when you turn the shield off.

Select **Options** to open the contextual menu or **Back** to return to the main screen.



7.4.1. Shield Menu

If you select **Options**, a contextual menu will appear. The following commands are available:

- **Help** - to access the contextual help file.
- **Exit** - to exit the application.

7.4.2. Configuring the Shield

To turn real-time protection on / off, select **Shield status**. By selecting this option, a new screen will appear.

Two options are available:

Option	Description
On	Turns on real-time protection.
Off	Turns off real-time protection.

Choose the desired option and select **OK**. If you want to return to the previous screen without making any changes, select **Cancel**.

Shield Status

Initially, the shield is turned off. The first time you turn on the shield you will have to restart your device.

Select **Yes** to restart your device and activate the shield. If you select **No**, the shield will remain turned off.

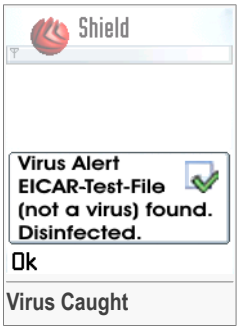
Warning

Activate the shield to protect your device from malware!

Activating the Shield

If enabled, the shield will permanently monitor your device, preventing the execution of infected files. When an infected file is detected, an alert will appear informing you about the infection.

Select **OK** to close the alert message.



Virus Caught

7.5. Update

To access this section choose **Update** from the main menu.

This is where you can initiate the update via device and view update information (the date and time of the last successful update and the update status).

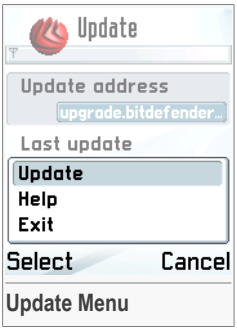
Select **Options** to open the contextual menu or **Back** to return to the main screen.

To see when the last successful update was performed, select **Last update**. A new screen will appear, where you can view this information.

7.5.1. Update Menu

If you select **Options**, a contextual menu will appear. The following commands are available:

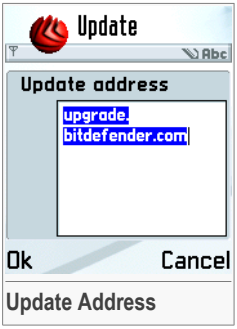
- **Update** - to update BitDefender via the device.
- **Help** - to access the contextual help file.
- **Exit** - to exit the application.



7.5.2. Setting the Update Address

To change the url address of the update server select **Update address**. By selecting this option, an edit box will appear.

Provide the new update server location and select **OK**. If you want to return to the previous screen without making any changes, select **Cancel**.



Note

The default location is `upgrade.bitdefender.com`.
Do not start the url address with "http://"; provide solely the server name. Otherwise, when updating via the device an error message will appear and BitDefender will fail to update.

7.5.3. Updating BitDefender

There are two ways of updating BitDefender:

- Update via Device
- Update via PC

Update via Device

BitDefender can be updated anytime you want by connecting to the Internet directly from the device. The process consists of downloading the update file on the mobile device from the update server and reinstalling the application on the device.

Important

To connect via GPRS, make sure the GPRS service is activated and the appropriate settings are installed on your device. If not, contact your mobile phone operator in order to activate GPRS and to receive the GPRS settings.

Follow these steps to update BitDefender via the device:

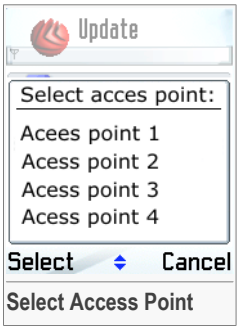
1. Set the address of the update server. For more information, check "*Setting the Update Address*" (p. 65).

   Note

   This step is optional!

2. Select **Update** from the Update menu.

   After a few seconds, a screen will appear containing a list of access points:



3. Select an access point.

   Note

   You can connect to the Internet via GPRS using the access point given by your operator or through a wireless connection.

   BitDefender will connect to the update server and download the update file on the device.

4. Once the update file has been transferred on your device, BitDefender will be closed and the installer will start. Follow the on-screen instructions on your device to reinstall the updated application.

   Note

   For detailed information about the installation steps on your device, check "*Install*" (p. 14).

5. If the update was successful, a message will appear. Select **OK** to restart the application.

Update via PC

BitDefender can be updated using the desktop application. The process consists of downloading the update file on an Internet-connected computer, transferring it to the mobile device and reinstalling the application on the device.

Important

Nokia PC Suite must be installed on your computer in order to update BitDefender Mobile Security via PC.

Follow these steps to update BitDefender via PC:

1. Connect the device to the PC (through Bluetooth™, infrared or cable) and make sure that the Nokia PC Suite detects it.
2. Download the update file to the PC using the desktop application (in the Update section, click **Update**).

   The desktop module will connect to the device, download the update file on your computer and transfer it on your device

   Note

   If the device is not connected to the PC or if the product is not valid, the update process will be cancelled.

3. Once the update file has been transferred on your device, BitDefender will be closed and the installer will start. Follow the on-screen instructions on your device to reinstall the updated application.

   Note

   For detailed information about the installation steps on your device, check "*Install*" (p. 14).

4. If the update was successful, a message will appear. Select **OK** to restart the application.

Note

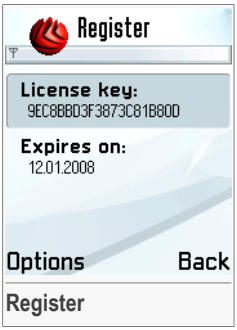
For more information about the desktop application, check the BitDefender Mobile Security - Update Module chapter of this user guide.

7.6. Register

To access this section choose **Register** from the main menu.

This is where you can register the product and see the current BitDefender license key and its expiration date.

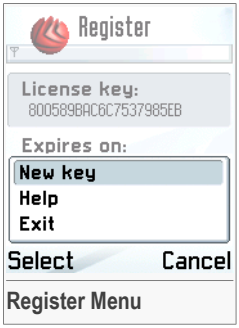
Select **Options** to open the contextual menu or **Back** to return to the main screen.



7.6.1. Register Menu

If you select **Options**, a contextual menu will appear. The following commands are available:

- **New key** - to register the product.
- **Help** - to access the contextual help file.
- **Exit** - to exit the application.



Register Menu

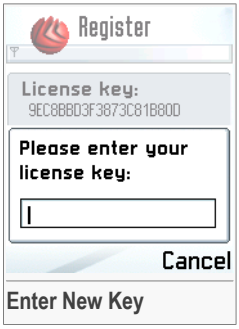
7.6.2. Registering BitDefender Mobile Security

To register the product or change the license key select **New key** from the Register menu. A dialog will appear.

Enter a valid license key and select **OK**.

Important
The license key is a 20-character alphanumerical string!

If you want to return to the **Register** section without changing the license key, select **Cancel**.



Enter New Key

8. Symbian S80 Devices

The **Symbian S80 Devices** chapter of this user guide contains the following topics:

- Overview
- Scan
- Report
- Shield
- Update
- Register

8.1. Overview

BitDefender Mobile Security is the application installed on your mobile device so as to protect it against viruses and other malware.

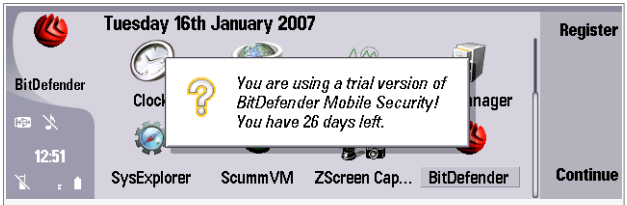
8.1.1. Getting Started

To start BitDefender, browse for the **BitDefender icon** in the phone menu and then either press the action button or use the **Open** command. If you are using a registered version, the main screen will be displayed.

If you are using a trial version, each time you open **BitDefender Mobile Security**, you will be requested to register the product.

Important

This also happens if the product has expired or is about to expire (the last 3 days of the licensing period).

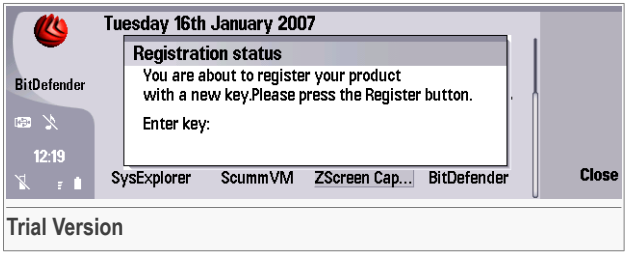


Trial Version

Two commands are available:

- **Register** - to register the product.
- **Continue** - to continue evaluating the product.

If you choose **Register**, a message asking you to enter the license key will appear.



Provide a valid license key and select **Continue** to use the registered version.

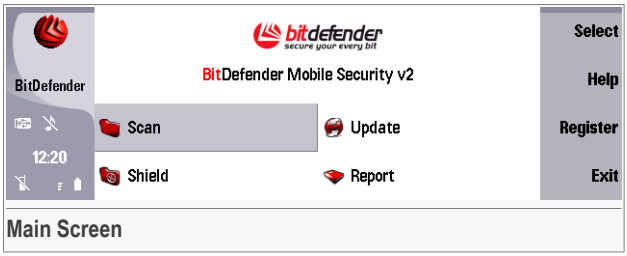
Important
The license key is a 20-character alphanumerical string!

Select **Close** to continue evaluating the product.

If you choose **Continue**, the main screen will be displayed. If you decide to register the product later during the session, you can do that in the Register section.

8.1.2. Main Screen

This is where you get access to all BitDefender sections.



The following options are available:

- **Scan** - to access the **Scan** section.
- **Shield** - to access the **Shield** section.

- **Update** - to access the **Update** section.
- **Report** - to access the **Report** section.

Note

To find more information about each section, check the corresponding section in this chapter.

Use the **Select** command or the navigation button to open a section.

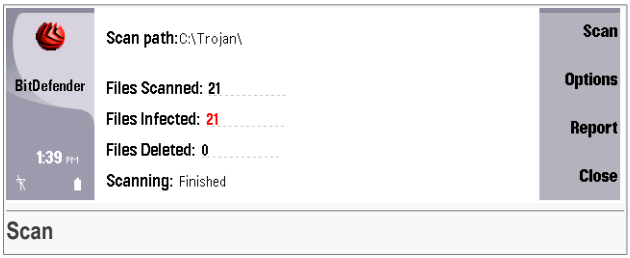
To access the **Register** section use the **Register** command.

To access the help file use the **Help** command. Each section has a contextual help. Press `H` or `Chr+?` to access the contextual help.

You can exit the application by using the **Exit** command.

8.2. Scan

To access this section choose **Scan** from the main screen.



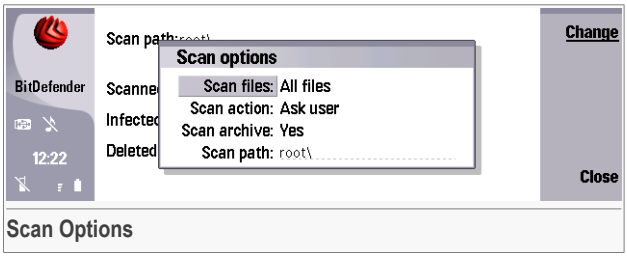
This is where you can configure **BitDefender Mobile Security** to scan your device and you can see scan information (the scan path, the number of scanned / infected / deleted files for the current / last scan event).

8.2.1. Configuring the Scan Options

Important

By default, BitDefender will scan all your files, except for archives, and prompt you for action.

Before initiating a scan you may want to set the scan options. Use the **Options** command to access the **Scan options** section, where you can specify the scan settings.



Scan Options

You can configure the following scan options:

- **Scan files** - to specify the type of files to be scanned.

  Two options are available:

Option	Description
All files	All files will be scanned for viruses and other malware.
Only programs	Only program files will be scanned for viruses and other malware. This means that only the files with an `.exe`, `.app` and `.dll` extension will be scanned.

  Use the navigation button to modify this setting.

  Note

  You can also use the **Change** command. Choose the desired option from the submenu and select **OK**. If you want to return to the previous screen without making any changes, select **Cancel**.

- **Scan action** - to specify the action mode.

  Three options are available:

Option	Description
Ask user	When an infected file is found, BitDefender prompts the user for action. You must confirm your choice: delete / ignore only the infected file (**Yes / No**) or all the infected files (**Yes to all / No to all**).
Delete	Infected files will be automatically deleted.
None	Infected files will be ignored.

Use the navigation button to modify this setting.

Note

You can also use the **Change** command. Choose the desired option from the submenu and select **OK**. If you want to return to the previous screen without making any changes, select **Cancel**.

- **Scan archives** - to specify whether to scan inside archives or not.

  Two options are available:

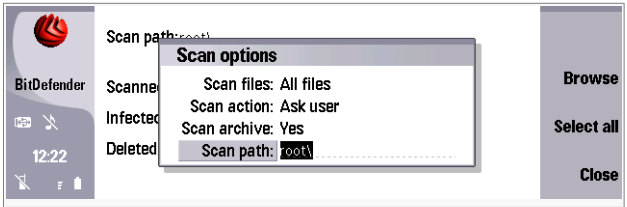
Option	Description
No	Archives will not be scanned.
Yes	Archives will be scanned.

Use the navigation button to modify this setting.

Note

You can also use the **Change** command. Choose the desired option from the submenu and select **OK**. If you want to return to the previous screen without making any changes, select **Cancel**.

- **Scan path** - to specify the scan target. If you select this option, you will be able to edit the scan path. Also, several other commands will appear on the screen.



Modify the Scan Path

Provide the path to the files or folders you want to be scanned.

Important

Every path you type must end in a **backslash "\"** to be valid. Otherwise, when you start a scan process an error message will appear and the scan will be cancelled.

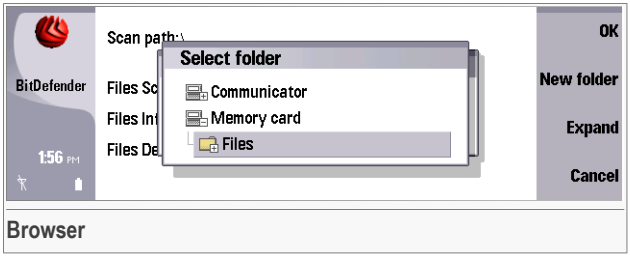
Note

The default path is: `root\`. With this option, all your files will be scanned.

Use the **Select all** command to set BitDefender to scan all memory.

An easier method to specify the scan target is to use the browser:

1. Use the **Browse** command to open the browser. A new screen will appear, containing a list of all available memory types.



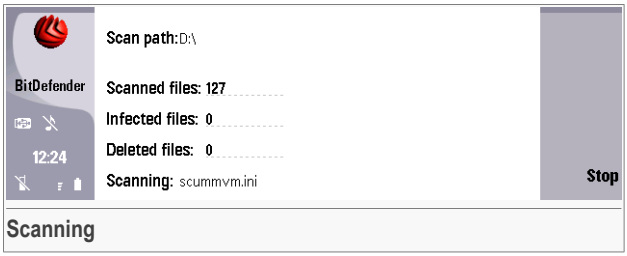
2. Use the navigation button to browse through folders and find the scan target. To expand / collapse objects that contain subfolders you can also use the commands **Expand / Collapse**.
3. Select **OK** to set the new path and return to the scan options. The new path will appear in the **Scan path** field.

   To return to the previous screen without making any changes select **Cancel**.

Use the **Close** command to return to the **Scan** section.

8.2.2. Scanning the Device

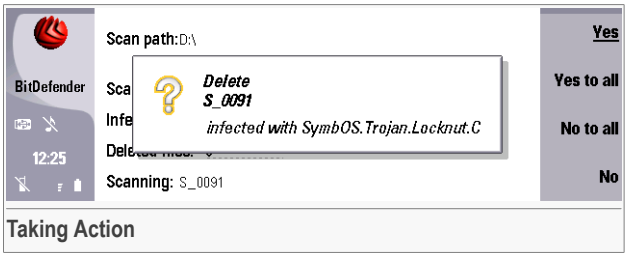
To initiate the scanning process, select the **Scan** command. A new screen will appear where you can see details about the files that are being scanned.



You can see the last file scanned. If an infected file is detected, depending on the scan action selected, it will be automatically deleted, ignored or you will be prompted for action.

The scanning process can be cancelled at any moment by selecting **Stop**.

If the **Ask user** option is enabled, you will be prompted for action everytime an infected file is detected. A message asking you to delete the infected file will appear.



Choose a command to apply the desired action:

- **Yes** - to delete the infected file;
- **Yes to All** - to delete all infected files;
- **No to All** - to ignore every infected file;
- **No** - to ignore the infected file.

Warning

If you choose **No** or **No to All**, your system will not be protected.

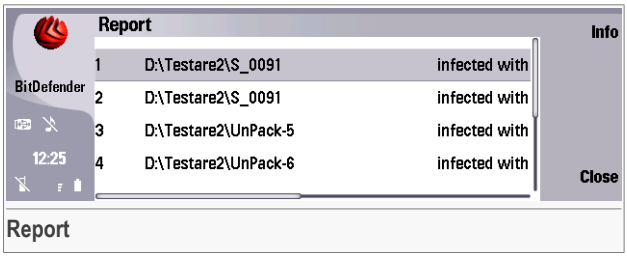
At the end of the scanning process, you will be directed to the Report section where you can view the scan results.

8.3. Report

To access this section choose **Report** from the main screen.

Note

At the end of each scanning process, you will be directed to this section to view the scan results.



This is where you can see the list of all of the infected files detected during the last successful scan. The path, the name of the virus and the disinfection status are provided for each file.

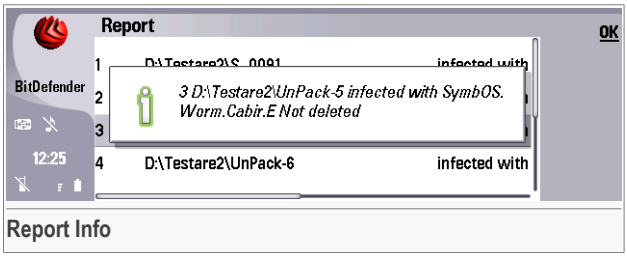
Note

If no virus was detected the message *No virus found* will appear instead.

Use the **Close** command to return to the previous section.

8.3.1. Viewing the Scan Results

To see all information about an infected file selected use the **Info** command. A message containing information about the selected item will appear.

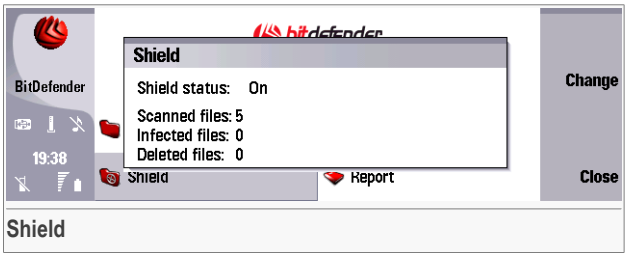


You can see the filename and its path, the name of the virus and the disinfection status.

Select **OK** to return to the Report section.

8.4. Shield

To access this section choose **Shield** from the main screen.



Shield

This is where you can enable / disable real-time protection and view the shield statistics.

You can see the number of scanned / infected / disinfected files per session. A session starts when you turn the shield on and it ends when you turn the shield off.

Use the **Close** command to return to the main screen.

8.4.1. Configuring the Shield

To turn real-time protection on / off use the **Change** command.

Initially, the shield is turned off. The first time you turn on the shield you will have to restart your device.

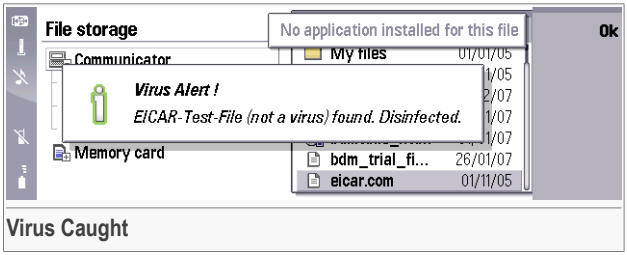
Activating the Shield

Select **OK** to restart your device and activate the shield. If you select **Cancel**, the shield will remain turned off.

Warning

Activate the shield to protect your device from malware!

If enabled, the shield will permanently monitor your device, preventing the execution of infected files. When an infected file is detected, an alert will appear informing you about the infection.

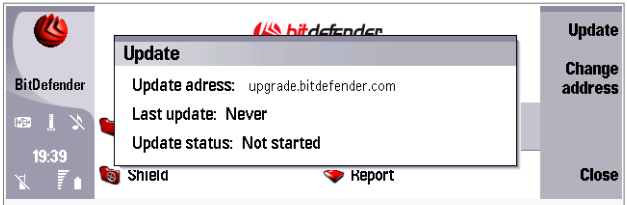


Virus Caught

Select **OK** to close the alert message.

8.5. Update

To access this section choose **Update** from the main screen.



Update

This is where you can initiate the update via device and view update information (the date and time of the last successful update and the update status).

Use the **Close** command to return to the main screen.

8.5.1. Setting the Update Address

To change the url address of the update server select the **Change address** command. Enter the new location in the edit field.

Note

The default location is `upgrade.bitdefender.com`.
Do not start the url address with "http://"; provide solely the server name. Otherwise, when updating via the device an error message will appear and BitDefender will fail to update.

8.5.2. Updating BitDefender

There are two ways of updating BitDefender:

- Update via Device
- Update via PC

Update via Device

BitDefender can be updated anytime you want by connecting to the Internet directly from the device. The process consists of downloading the update file on the mobile device from the update server and reinstalling the application on the device.

Important

To connect via GPRS, make sure the GPRS service is activated and the appropriate settings are installed on your device. If not, contact your mobile phone operator in order to activate GPRS and to receive the GPRS settings.

Follow these steps to update BitDefender via the device:

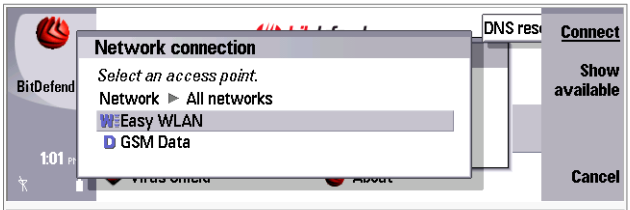
1. Set the address of the update server. For more information, check "*Setting the Update Address*" (p. 65).

   Note

   This step is optional!

2. Select the **Update** command.

   After a few seconds, a screen will appear containing a list of access points:



Select Access Point

3. Select an access point (using the action button or the **Connect** command). Use the **Show all / Show available** commands to see all or only the available access points.

Note

You can connect to the Internet via GPRS using the access point given by your operator or through a wireless connection.

BitDefender will connect to the update server and download the update file on the device.

4. Once the update file has been transferred on your device, BitDefender will be closed and the installer will start. Follow the on-screen instructions on your device to reinstall the updated application.

Note

For detailed information about the installation steps on your device, check "*Install*" (p. 14).

5. If the update was successful, a message will appear. Select **OK** and restart the application.

Update via PC

BitDefender can be updated using the desktop application. The process consists of downloading the update file on an Internet-connected computer, transferring it to the mobile device and reinstalling the application on the device.

Important

Nokia PC Suite must be installed on your computer in order to update BitDefender Mobile Security via PC.

Follow these steps to update BitDefender via PC:

1. Connect the device to the PC (through Bluetooth™, infrared or cable) and make sure that the Nokia PC Suite detects it.
2. Download the update file to the PC using the desktop application (in the Update section, click **Update now**).

   The desktop module will connect to the device, download the update file on your computer and transfer it on your device

Note

If the device is not connected to the PC or if the product is not valid, the update process will be cancelled.

3. Once the update file has been transferred on your device, BitDefender will be closed and the installer will start. Follow the on-screen instructions on your device to reinstall the updated application.

Note

For detailed information about the installation steps on your device, check "*Install*" (p. 14).

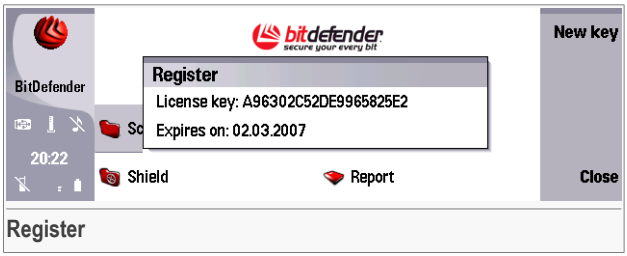
4. If the update was successful, a message will appear. Select **OK** and restart the application.

Note

For more information about the desktop application, check the BitDefender Mobile Security - Update Module chapter of this user guide.

8.6. Register

To access this section use the **Register** command from the main menu.



This is where you can register the product and see the current BitDefender license key and its expiration date.

Use the **Close** command to return to the main screen.

8.6.1. Registering BitDefender Mobile Security

To register the product or change the license key select **New key** command. A dialog will appear.

Enter a valid license key and select **OK**.

Important

The license key is a 20-character alphanumerical string!

If you want to return to the **Register** section without changing the license key, select **Close**.

9. BitDefender Mobile Security - Update Module

The **BitDefender Mobile Security - Update Module** chapter of this user guide contains the following topics:

- Overview
- Update
- Settings
- Help

9.1. Overview

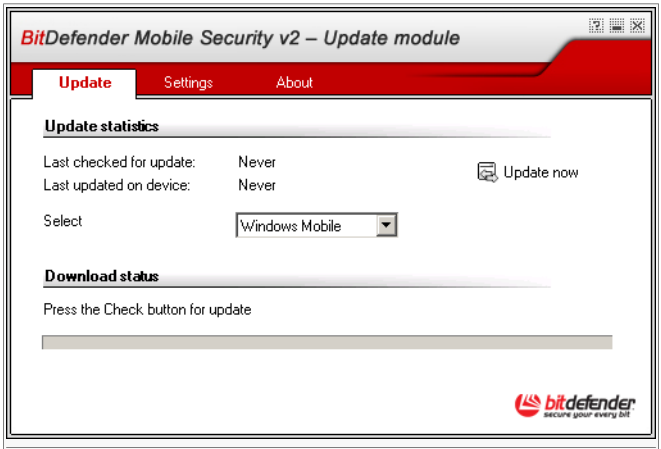
BitDefender Mobile Security - Update Module represents the desktop component of **BitDefender Mobile Security**. Its function is to help you install BitDefender Mobile Security on your device and to update it, as well as to provide complete user support.

Important

During the installation of **BitDefender Mobile Security - Update Module**, the installation package for **BitDefender Mobile Security** will be automatically sent to your mobile device and then the installation process will start.

9.1.1. Getting Started

To access the console of the desktop module, follow the path: **Start** → **Programs** → **BitDefender** → **BitDefender Mobile Security** or quicker, double click the **BitDefender icon** from the system tray.



Desktop Module

The desktop console contains the following sections:

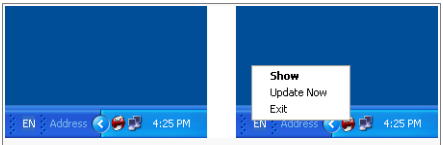
- Update - in this section you can initiate the update process via PC of BitDefender Mobile Security.
- Settings - in this section you can configure the settings of the desktop module.
- Help - in this section you can find contact and technical support information.

To access a section click the corresponding tab.

To learn more about the product, its features and how to use it, open the help file by clicking ? (the question mark) in the upper right corner.

9.1.2. BitDefender Icon in System Tray

When the console is minimized, an icon will appear in the system tray:

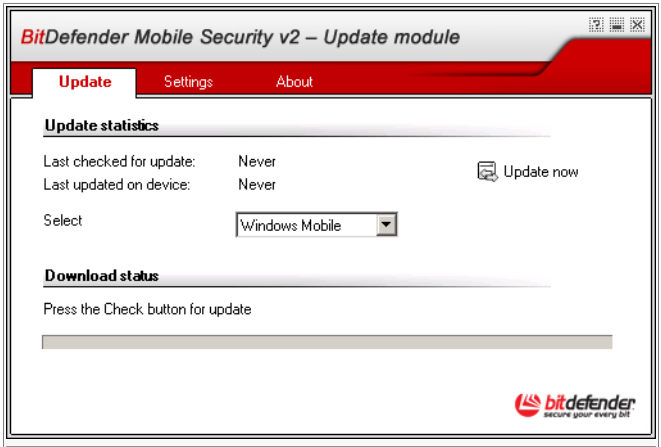


BitDefender Icon in System Tray

If you double-click this icon, the console will open. Also, by right-clicking it, a contextual menu containing the following options will appear:

- **Show** - opens the console.
- **Update now** - initiates the update via PC.
- **Exit** - shuts down the application. By selecting this option, the icon in the system tray will disappear and in order to access the console, you will have to launch it again from the Windows Start menu.

9.2. Update



Update

This is where you can check for updates and see update statistics. You can see the date and time of the last check and last successful update.

9.2.1. Updating BitDefender

BitDefender can check for updates from the local network, over the Internet, directly or through a proxy server.

In order to update **BitDefender Mobile Security** via PC, you must download the updates on your computer. To check for updates follow these steps:

1. Select the operating system your device works on: **Symbian OS** or **Windows Mobile**.

2. Connect the device to the PC.
3. Click **Update Now**.

Note

If you are connected to the Internet through broadband or DSL, you can set BitDefender to automatically check for updates whenever the device is connected to the PC by selecting **Automatically update when device is connected** in the Settings section.

If the device is connected to the PC, BitDefender will connect to the update server and check if the product is valid. If the product is valid, BitDefender will first check for updates available for the desktop module. If any, the console will be updated and then BitDefender will resume the check for updates for BitDefender Mobile Security.

If an update was detected, it will be downloaded to your computer. BitDefender will automatically transfer the update file on your device using Nokia PC Suite for Symbian devices or ActiveSync for Windows Mobile devices.

Note

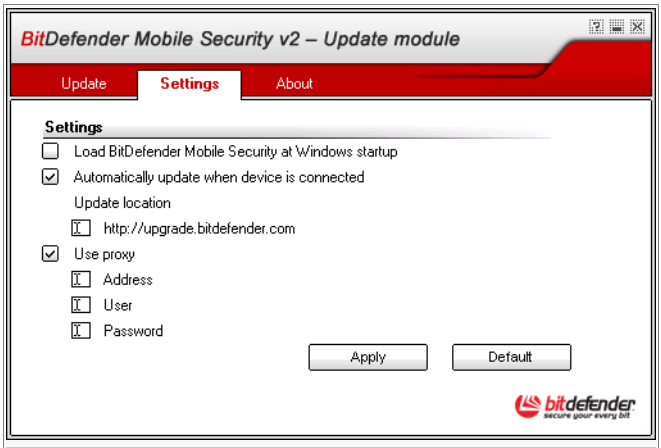
If the connection times out, the update file will not be sent to your device and BitDefender Mobile Security will not be updated.

Follow the on-screen instructions on your device in order to complete the update process.

Note

Check the "*Install*" (p. 14) section to learn how to complete the update process.

9.3. Settings



Settings

This is where you can configure the desktop module settings.

The following options are available:

- **Load BitDefender Mobile Security at Windows startup** - automatically launch BitDefender Mobile Security at startup.
- **Automatically update when device is connected** - automatically check for available updates at the specified update location when the device is connected to the computer.
- **Update location** - in this edit field you can specify the location where BitDefender should check for updates. The default location is: http://upgrade.bitdefender.com.

  Note

  This is useful for example if you are connected to a local network that has BitDefender virus signatures placed locally.

- **Use proxy** - check this option if you use a proxy server to connect to the Internet. The following settings must be specified:
  - **Address** - type in the IP or the name of the proxy server and the port BitDefender uses to connect to the proxy server.

Important

Syntax: `name:port` or `ip:port`.

- **User** - type in a user name recognized by the proxy.

Important

Syntax: `domain\user`.

- **Password** - type in the valid password for the previously specified user.

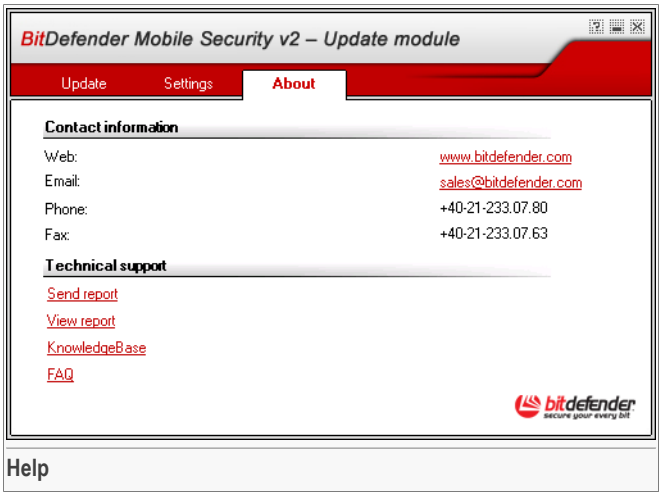
Note

The proxy settings appear only if you enable the **Use proxy** option.

To enable / disable an option select / clear the corresponding check box.

Click **Apply** to save the changes. If you click **Default**, the default settings will be restored.

9.4. Help



Help

This is where you can get all the information you need in case something unexpected appears. Also, here you can find contact information.

9.4.1. Contact Information

To learn more about BitDefender or to contact us, use the information under the **Contact Information** heading.

9.4.2. Technical Support

Every time an update check is requested, no matter if it is manual or automatic, a report file is created. To see the report file, click **View report**.

If something goes wrong during the update, you can send the report file to BitDefender by clicking **Send report**. Also, if you have any problem using the product, click this link and explain the problem in detail.

To learn more about the product, its features and how to use it, open the help file by clicking ? (the question mark) in the upper right corner. Also, you are welcome to search our online Knowledge Base by clicking **Knowledge Base** and our online FAQ database by clicking **FAQ**.

Important

An active Internet connection is required in order to access the **online Knowledge Base** or the **online FAQ database**.

Note

For more information please check the "*Support*" (p. 93) chapter of this user guide.

Getting Help

10. Support

10.1. Support Department

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

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

You are welcome to ask for support at <support@bitdefender.com> at any time. For a prompt response, please include in your email as many details as you can about your BitDefender, your system and describe the problem you have encountered as accurately as possible.

10.2. On-line Help

10.2.1. BitDefender Knowledge Base

The BitDefender Knowledge Base is an online repository of information about the BitDefender products. It stores, in an easily accessible format, reports on the results of the ongoing technical support and bugfixing activities of the BitDefender support and development teams, along with more general articles about virus prevention, the management of BitDefender solutions with detailed explanations, and many other articles.

The BitDefender Knowledge Base is open to the public and freely searchable. The extensive information it contains is yet another means of providing BitDefender customers with the technical knowledge and insight they need. All valid requests for information or bug reports coming from BitDefender clients eventually find their way into the BitDefender Knowledge Base, as bugfix reports, workaround cheatsheets or informational articles to supplement product helpfiles.

The BitDefender Knowledge Base is available any time at http://kb.bitdefender.com.

10.3. Contact Information

Efficient communication is the key to a successful business. During the past 10 years SOFTWIN has established an unquestionable reputation by constantly striving for better communication so as to exceed the expectations of our clients and partners. Should you have any questions, do not hesitate to contact us.

10.3.1. Web Addresses

Sales department: <sales@bitdefender.com>
Technical support: <support@bitdefender.com>
Documentation: <documentation@bitdefender.com>
Partner Program: <partners@bitdefender.com>
Marketing: <marketing@bitdefender.com>
Media Relations: <pr@bitdefender.com>
Job Opportunities: <jobs@bitdefender.com>
Virus Submissions: <virus_submission@bitdefender.com>
Spam Submissions: <spam_submission@bitdefender.com>
Report Abuse: <abuse@bitdefender.com>
Product web site: http://www.bitdefender.com
Product ftp archives: ftp://ftp.bitdefender.com/pub
Local distributors: http://www.bitdefender.com/partner_list
BitDefender Knowledge Base: http://kb.bitdefender.com

10.3.2. Branch Offices

The BitDefender offices are ready to respond to any inquiries regarding their areas of operation, both in commercial and in general matters. Their respective addresses and contacts are listed below.

Germany

Softwin GmbH
Headquarter Western Europe
Karlsdorferstrasse 56
88069 Tettnang
Germany
Tel: +49 7542 9444 44
Fax: +49 7542 9444 99
Email: <info@bitdefender.com>
Sales: <sales@bitdefender.com>

Web: http://www.bitdefender.com
Technical Support: <support@bitdefender.com>

UK and Ireland

One Victoria Square
Birmingham
B1 1BD
Tel: +44 207 153 9959
Fax: +44 845 130 5069
Email: <info@bitdefender.com>
Sales: <sales@bitdefender.com>
Web: http://www.bitdefender.co.uk
Technical support: <support@bitdefender.com>

Spain

Constelación Negocial, S.L
C/ Balmes 195, 2a planta, 08006
Barcelona
Soporte técnico: <soporte@bitdefender-es.com>
Ventas: <comercial@bitdefender-es.com>
Phone: +34 932189615
Fax: +34 932179128
Sitio web del producto: http://www.bitdefender-es.com

U.S.A

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Technical support:
Email: <support@bitdefender.com>
Customer Service: 954-776-6262
http://www.bitdefender.com

Romania

SOFTWIN
5th Fabrica de Glucoza St.
PO BOX 52-93
Bucharest
Technical support: <suport@bitdefender.ro>

Sales: <sales@bitdefender.ro>
Phone: +40 21 2330780
Fax: +40 21 2330763
Product web site: http://www.bitdefender.ro

Glossary

Access point

An access point is a stand alone device used to connect wireless communication devices in its range to a fixed wire network. Using this base station, a mobile device owner can connect to other mobile device or computer, to the Internet or to a server.

It also refers to the radio device atached to the mobile device that receives the signal from the base station.

Backdoor

A hole in the security of a system deliberately left in place by designers or maintainers. The motivation for such holes is not always sinister; some operating systems, for example, come out of the box with privileged accounts intended for use by field service technicians or the vendor's maintenance programmers.

Bluetooth

It represents a short-range radio technology which enables a low cost, low power wireless connection. A device that supports bluetooth can connect to one or more bluetooth supporting devices only if they are in range and the connection is accepted by each part. The most common range of action for a such device is 10 metres.

Two devices using bluetooth connection can easily trasfer data. Although manufacturers and developers have taken many security measures to protect the system and the data, it doesn't mean that there is no security risk. However, without specialised equipment, a potential attack can be launched only if the hacker's device is in range.

Browser

Generally, a software application used to locate and display files or folders. It is most commonly used when reffering to Internet. A web browser is used to locate and display Web pages.

Disk drive

It's a machine that reads data from and writes data onto a disk.

Download

To copy data (usually an entire file) from a main source to a peripheral device. The term is often used to describe the process of copying a file from an online service to one's own computer or mobile device. Downloading can also refer to copying a file from a network file server to a computer on the network.

E-mail

Electronic mail. A service that sends messages on computers via local or global networks.

Error messages

Whenever BitDefender encounters an error or doesn't function properly, an error message will be displayed. It contains information about what had gone wrong.

Events

An action or occurrence detected by a program. Events can be user actions, such as clicking a mouse button or pressing a key, or system occurrences, such as running out of memory.

Filename extension

The portion of a filename, following the final point, which indicates the kind of data stored in the file.

Many operating systems use filename extensions, e.g. Unix, VMS, and MS-DOS. They are usually from one to three letters (some sad old OSes support no more than three). Examples include "c" for C source code, "ps" for PostScript, "txt" for arbitrary text.

GPRS

General Packet Radio Service (GPRS) is a mobile data service that enables sending and receiving data at a moderate speed. It is commonly used for sending and receiving emails and MMS messages, web browsing, downloading games, ringtones or logos etc.

Infrared

Infrared radiation is an electromagnetic radiation that has wavelengths situated between 750nm and 1mm. One of its main use is enabling short-range communication between computers, computer peripherals and mobile devices.

Data can be easily exchanged using infrared devices. Unlike bluetooth technology, the infrared connection permits a secure data transfer.

I/O errors

An I/O error is counted everytime the scanning engine is denied access to a file. The files for which an I/O error is returned include the operating system files, the files in use, and the user-protected files.

Operating system files. The files are in use by the Windows operating system and the scanning engine is permanently denied access to them. For example, the paging file used for storing the system virtual memory is inaccessible to the antivirus.

Files in use. The files are in use by other software and the scanning engine is temporarily denied access to them. For example, using an editing software during a scan will deny the access to the files opened in the editing software. Closing the editing software before starting the scan will allow the scanning engine to access these files.

User-protected files. The user initiating the scan is denied the access to the files. For example, although a user is allowed to scan the files contained in her home folder on a file server, she will not be able to scan the files from the other users' home folders stored on the same file server.

To reduce the number of I/O errors, close all other software before intiating the scan.

Malware

Short for malicious software. The term refers to any application designed to damage a system.

This kind of software comprises a various range of different applications, such as viruses, trojans and worms.

Memory

Internal storage areas in the computer or the mobile device. The term memory identifies data storage that comes in the form of chips, while the word storage is used for memory that exists on tapes or disks.

A mobile device has three types of memory: RAM, ROM and flash. RAM represents the read and write memory, while ROM is the read-only memory. The data stored in RAM can be modified and, when the power is turned off, it is lost. In ROM, the data cannot be modified or erased. Flash memory is a memory chip where a program can be stored. It can be erased and reprogramed in blocks, but only in special conditions.

To extend the memory of a device, a MMC can be used. MMC, or Multi Media Card, is a flash memory card. Its size can reach up to 2 Gb.

MMS

Multimedia Message Service(SMS) is a service that permits the sending of multimedia content from a mobile device to another using WAP technology. Images, audio or video clips can be sent via MMS.

A mobile device can be infected using this service, by receiving an infected file.

Mobile device

Currently, it is used when reffering to intelligent mobile communication devices, such as smartphones and handhels devices. Running on operating systems,

combining phone and computer features and small size are their main characteristics.

Path

The exact directions to a file on a device that works on an operating system. These directions are usually described by means of the hierarchical filing system from the top down.

The route between any two points, such as the communications channel between two computers.

Port

An interface on a computer to which you can connect a device. Personal computers have various types of ports. Internally, there are several ports for connecting disk drives, display screens, and keyboards. Externally, personal computers have ports for connecting modems, printers, mice, bluetooth device, infrared device and other peripheral devices.

In TCP/IP and UDP networks, an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.

Report file

A file that lists actions that have occurred. BitDefender maintains a report file that contains the scan results.

Root

Represents the top level of a hierarchy.

When talking about the disk drive root, it refers to all files or folders.

SMS

Short Message Service(SMS) is a service available on most mobile phones. It enables two mobile phones owners to communicate through short text messages.

Startup items

Any files placed in this folder will open when the computer starts. For example, a startup screen, a sound file to be played when the computer first starts, a reminder calendar, or application programs can be startup items. Normally, an alias of a file is placed in this folder rather than the file itself.

System tray

Introduced with Windows 95, the system tray is located in the Windows taskbar (usually at the bottom next to the clock) and contains miniature icons for easy access to system functions such as fax, printer, modem, volume, and more. Double click or right click an icon to view and access the details and controls.

Trojan

A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. However, they may contain a package with several malicious applications, like viruses or worms, that can spread by themselves and affect other mobile devices or even computers. One of the most insidious types of Trojan horse is a program that claims to rid your device of viruses but instead introduces viruses onto your device.

The term comes from a story in Homer's Iliad, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

Update

A new version of a software or hardware product designed to replace an older version of the same product. In addition, the installation routines for updates often check to make sure that an older version is already installed on your device; if not, you cannot install the update.

BitDefender has it's own update module that allows you to manually check for updates, or let it automatically update the product.

Virus

A program or piece of code that is loaded onto your device without your knowledge and runs against your will. Most viruses can also replicate themselves. A simple virus that can copy itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

Virus definition

The binary pattern of a virus, used by the antivirus program to detect and eliminate the virus.

WAP

Wireless Application Protocol (WAP) is a system similar to a Web browser designed for applications that run on mobile devices. Internet access from a mobile device is possible thanks to WAP technology.

Worm

A malicious program that propagates itself over a network, reproducing itself as it goes. Mobile worms can spread from a mobile device to another via bluetooth or memory cards. Also, it can infect computers. It cannot attach itself to other programs.