BitDefender Client Security
Maximum Value for Your Security Needs

EVALUATOR'S GUIDE

bitdefender

Summary

bitdefender

1. Quick Summary

BitDefender Client Security	
TAG LINE	Proactive Security and Management
CLIENT PLATFORMS	Windows 2000 Prof.+SP4 and Update Rollup 1 v.2,
	Windows XP+SP2 (32/64bit),
	Windows Vista (32/64 bit)
	Windows 7 (32/64 bit)
SERVER PLATFORMS	Windows 2000 Professional + SP4
	Windows 2000 Server + SP4
	Windows XP + SP2 (32/64bit)
	Windows Server 2003 + SP2(32/64bit)
	Windows Server 2008(32/64bit)
	Windows Vista (32/64 bit)
	Windows 7 (32/64 bit)
	Database: Microsoft SQL Server 2005 / SQLExpress
DESCRIPTION	BitDefender Client Security is a robust and easy-to-use business security and management solution that delivers superior proactive protection from viruses, spyware, rootkits, spam, phishing and other malware.
	BitDefender Client Security increases business productivity and reduces management and malware-related costs through its use of centralized administration, which allows for network-wide protection and control of individual workstations from a single endpoint.
AVAILABILITY	April 1st, 2008 (English version)
LANGUAGES	English, French, German, Spanish, Chinese Simplified, Japanese
LICENSE	The license includes:
	▪ Free technical support
	▪ Automatic virus definitions updates

	▪ Upgrade to any new version of the solution

bitdefender

2. Solution Description

BitDefender Client Security is a robust and easy-to-use business security and management solution that delivers superior proactive protection from viruses, spyware, rootkits, spam, phishing and other malware.

BitDefender Client Security increases business productivity and reduces management and malware-related costs through its use of centralized administration, which allows for network-wide protection and control of individual workstations from a single endpoint.

BitDefender Client Security offers two core modules in a single solution:

- **BitDefender Business Client**
  - Once installed on the company's workstations, it provides industry- leading proactive protection against viruses, spyware, rootkits, spam, phishing and other malware

- **BitDefender Management Server**
  - Automatically performs routine and recurrent activities for a more efficient network management
  - Ensures security compliance by applying consistent policies throughout the network
  - Manages and controls BitDefender Business Client and other BitDefender server solutions.
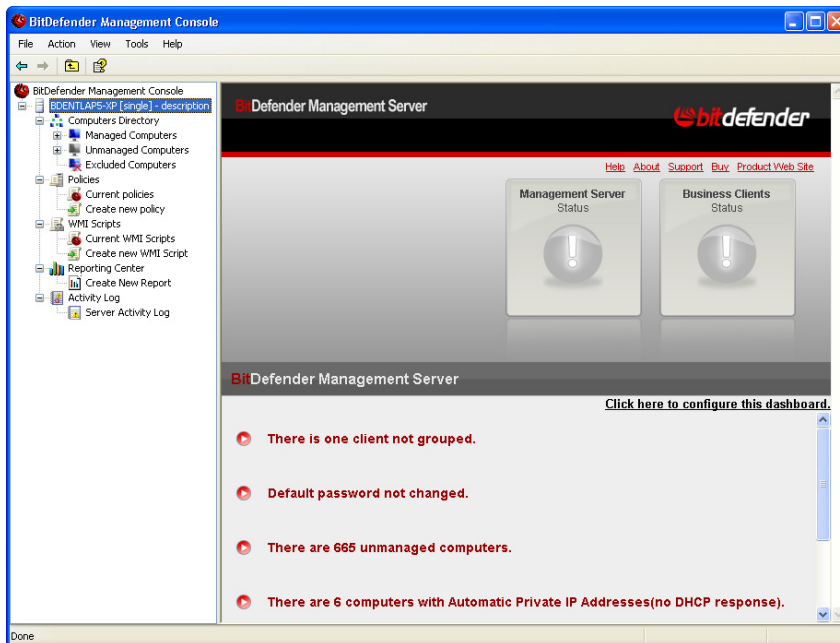

Fig.2.1 BitDefender Management Server – Dashboard Main View

3. Main Benefits and Features

Reduced Administration Workload and Costs

- Provides a series of configurable security policies which can be easily set using pre-defined templates
- Maintains mobile users' compliance with corporate security policies even while offline
- Integrates with Active Directory for an easy and flexible management process
- Helps address compliance issues related to network admission by automatically detecting new stations and deploying Business Client on them
- Ensures consistent antimalware protection across the organization through centralized management of the Business Client features: antivirus, firewall, antispam, update, privacy control and user control
- Enhances management capabilities through the use of WMI scripts:
  - Remove software, kill processes, restart or shutdown workstations,
  - Enable/disable autoruns, enable/disable USB mass storage
- Increases business productivity through user activity administration controls:
  - Sets restrictions against unsafe or undesirable Web sites and user level applications
  - Blocks e-mail messages based on key words
  - Limits Internet access for specific periods of time

Enterprise-Wide Network Visibility

The solution is designed to improve the administrator's capacity to assess network security and take action, where necessary, based on:

- An enhanced reporting tool for regular statistics on network issues
- E-mail alerts about important security events
- WMI administration scripts run on workstations or computer groups for easy network auditing (hardware and system information, startup programs, installed software) .
- A first page summary (dashboard) with network security highlights and easy fixes

Optimized for Business Environments

- Saves workstation and network resources due to its small memory footprint and optimized server-client communication

- Works in the most commonly used network types (Ethernet, VPN, remote, WiFi)

- Provides a scalable master-slave architecture capable of managing an increased number of clients connected to a headquarter network from different physical locations

- Allows the setting of two types of clients - power clients, with unrestricted access to the interface, and restricted clients, with limited access to the interface

Improved Business Client Security

| Benefits	BitDefender Business Client Features				
	Antivirus & Antispyware	Firewall & Antiphising	Antispam	User Control	Local Backup
Protects business workstations and mobile users from malware, wireless and Web attacks or fraud attempts	X	X		X	
Safe and efficient traffic of business e-mails	X	X	X	X	
Increases employee productivity			X	X	
Provides the possibility of backing up important data					X
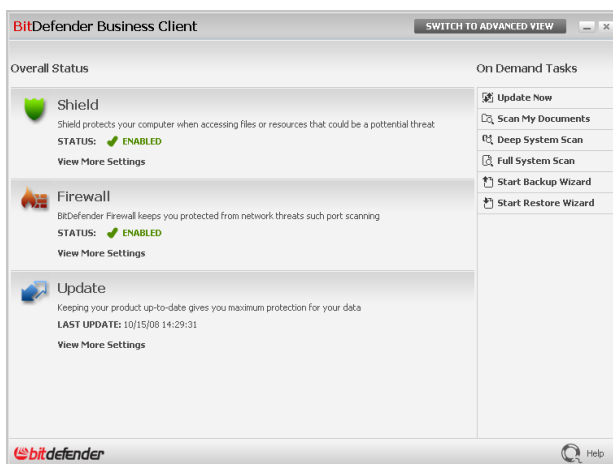
Fig. 3.1 BitDefender Business Client – Main Interface and Basic View

4. Services

Advanced Update System

- For continuous protection, BitDefender Client Security receives the latest updates and patches based on three configurable technologies: on-demand, scheduled and automatic.

Upgrades

- Registered users benefit from free upgrades to any new version of the solution during the license period. Special pricing is always provided to our customers when they renew their license, making BitDefender a long-term, cost effective solution.

Free 24/7 Professional Technical Support

- Certified representatives provide BitDefender business customers with free support on-line, by telephone or e-mail. This is supplemented by an on-line database with answers to Frequently Asked Questions and fixes for common issues.

5. System Requirements

BitDefender Management Server

• **Minimum processor:** Intel Pentium compatible processor 1GHz (2GHz recommended)

• **Minimum RAM memory:** 512MB (2MB recommended)

• **Minimum hard disk space:**
- 1.5GB (2.5GB recommended)
- For installation or upgrade 3GB are needed

• **Operating system:**
- Windows 2000 Professional with Service Pack 4
- Windows 2000 Server with Service Pack 4
- Windows XP with Service Pack 2
- Windows Server 2003 with Service Pack 2
- Windows Vista
- Windows 2008 Server
- Windows 7

• **Database:** Microsoft SQL Server 2005 / SQLExpress

BitDefender Agent

• **Minimum processor:** Intel Pentium compatible processor

- **Minimum RAM memory:**
  - 256MB RAM (512MB recommended) for Windows 2000, Windows XP, Windows 2003
  - 512MB RAM (1GB recommended) for Windows Vista, Windows 2008, Windows 7

- **Minimum hard disk space:** 100MB (200MB recommended)

- **Operating system:**
  - Windows 2000 Professional with Service Pack 4 and Update Rollup 1 Version 2
  - Windows 2000 Server with Service Pack 4
  - Windows XP with Service Pack 2
  - Windows Server 2003 with Service Pack 2
  - Windows Vista
  - Windows 2008 Server
  - Windows 7

BitDefender Management Console

- **Minimum processor:** Intel Pentium compatible processor (1GHz recommended)

- **Minimum RAM memory:**
  - 256MB RAM (512MB recommended) for Windows 2000
  - 512MB RAM (1GB recommended) for Windows XP, Windows 2003, Windows Vista, Windows 2008, Windows 7

- **Minimum hard disk space:**
  - 500MB (1GB recommended)
  - For installation or upgrade 2GB are needed

- **Operating system:**
  - Windows 2000 with Service Pack 4
  - Windows XP with Service Pack 2
  - Windows Server 2003 with Service Pack 2
  - Windows Vista
  - Windows Server 2008
  - Windows 7

- **Software:** Internet Explorer 6.0(+); Microsoft Management Console (MMC) 3.0(+)

- **Minimum resolution:** 1024x768 / 16 bit

BitDefender Business Client

- **Minimum processor:** Intel Pentium compatible processor 800MHz

- **Minimum RAM memory:**
  - 256MB RAM (512MB recommended) for Windows 2000

- 256MB RAM (1GB recommended) for Windows XP
- 512MB RAM (1GB recommended) for Window Vista, Windows 7

• **Minimum hard disk space:** 200MB (400MB for installation)

• **Operating system:**
- Windows 2000 Professional with Service Pack 4 and Update Rollup 1 Version 2
- Windows XP with Service Pack 2
- Windows Vista
- Windows 7

BitDefender Management Server installed together with BitDefender Business Client

• **Minimum processor:** Intel Pentium compatible processor 1.6GHz

• **Minimum RAM memory:**
- 756MB RAM (1GB recommended) for Windows 2000 and Windows XP
- 1GB RAM (2GB recommended) for Windows Vista and Windows 7

• **Minimum hard disk space:**
- 1.5GB (2GB recommended)
- For installation or upgrade 3GB are needed

• **Operating system:**
- Windows 2000 Professional with Service Pack 4
- Windows XP with Service Pack 2
- Windows Vista
- Windows 7

BitDefender Update Server

• **Supported browsers**
- Internet Explorer 6 (+) for Windows 2000
- Internet Explorer 7 (+) for Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows 2008 Server
- Mozilla Firefox 2.0 (+)

6. Technology Leadership

B-HAVE

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

NEUNET

- The new antispam filter available in BitDefender Total Security 2008 uses a Neural Network (a concept borrowed from the field of Artificial Intelligence) to deal with the new spam messages sent every day. Its main advantage is that it can recognize new spam by perceiving similarities (oftentimes very subtle) between the new messages received and the ones it was trained on.

Image Spam Filter

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

7. Test Recommendations

7.1. Client Security Basics

BitDefender Client Security has four main components:

- **BitDefender Management Server**, which allows you to centrally manage the BitDefender security solutions in your network.

- **BitDefender Management Console**, which is the graphical interface of BitDefender Management Server.

- **BitDefender Management Agent**, the local management component installed on all managed computers, which ensures communication between the managed computers and BitDefender Management Server.

- **BitDefender Business Client**, which protects workstations against a wide range of security threats. If you also want to protect servers and manage their protection, you must add support for the BitDefender server security solutions.

BitDefender Management Server centrally manages the following BitDefender products:

- BitDefender Business Client (included in the Client Security product);

- BitDefender Security for File Servers

- BitDefender Security for Exchange

- BitDefender Security for Mail Servers (UNIX, Win SMTP)

- BitDefender Security for Samba

7.2. Installation

BitDefender Management server can be installed as a single server or in a master-slave configuration for increased scalability. Three main scenarios are found more frequently:

- **Your network consists of less than 1000 computers.** This is the typical case in an SMB environment. In this case you install a single Management Server that manages all the clients in the network.

- **Your network consists of more than 1000 computers.** In this case, you divide the network into several subnetworks and install a BitDefender management server for each subnetwork. These are called slave servers. An additional management server will be installed in order to manage all slave servers. This is the master server.

- **Several networks from different geographical areas must be managed.** This is the typical case of businesses having offices in several cities or countries. In this case, you install a slave server in the network of each office. In the headquarter network, you install a slave server and a master server. The master server will manage all slave servers, including the slave server installed in the headquarter network.

These are the steps you must follow to successfully deploy BitDefender Client Security:

1. **Install the central management component** (BitDefender Management Server).

2. **Deploy the client management component** (BitDefender Management Agent) on the workstations and servers. This is done from the Management Console.

3. **Deploy workstation security** (BitDefender Business Client) on the client workstations. This is done from the management console. You just have to run a BitDefender Business Client policy on the workstations.

4. **Extending protection and management to servers.** To secure your organization's servers (Windows, file, mail servers etc) with BitDefender and to manage their protection using BitDefender Management Server, you must perform these additional steps:

   - Install the corresponding Server Add-ons

   - Install the server products

7.2.1. Install BitDefender Management Server

These are the quick steps to install Management Server:

1. *Choose* either **32 or 64 bit Management Server** from the **BitDefender Corporate Solution** Section.

2. *Run* the selected package and follow the **installation wizard.**

3. *Select* the **Setup type**

   - Default = All components

   - Custom = User selection

4. *Choose* the **Server Type**. If you are not using a multi server configuration, for typical installations use **Single**.

5. *Specify* the **Communication ports** (it's advisable to use the default if possible). If you choose a different set of ports make sure that the ports you have selected are open on the server machine.

6. *Choose* what database you want to use. You can choose either "**SQL Server Express**" or "**Use existing database**" (if you already have a working database that you want to use for the Management Server too).

7. If you choose the "**Install SQL Server Express**", the Management Server installation kit will install the SQL Express database on your computer. BitDefender generates a random password, which can be changed within the Management Console, under "**Tools**->**Change SQL password**".

8. If you choose the "**Use existing database**" option you need to provide a set of credentials (username and password) for BitDefender Management Server to be able to connect to the database.

9. *Connect* to database, press **Next.**

10. *Start* installation by pressing the **Install** button.

11. *Wait* until finished and then press **Finish.**

12. If you have other **BitDefender for server products** installed on your network, or if you are planning to install such products, and you want to be able to manage those products via the **Management Server**, you must *install* a **server add-on** component from the **BitDefender Corporate Solution**. Please note that you need the same installation files as your management server (either 32 or 64 bit). To install the server add-on you need to run the file, follow the prompts until it asks which software to install.

13. After you have finished installing *connect* to the **Management Server** (default credentials: Username: administrator, Password: admin)

7.2.2.   Deploy BitDefender Management Agent

There are 3 methods on deploying the Agents, choose the one most suitable to you. First you have to make sure the general conditions are met.

General Conditions:

1. *Configure* your **Credentials Manager** from "**Tools Menu**->**Credentials Manager**".

2. Make sure that the **Firewall** is disabled on the computers you want to deploy on.

3. If the **Management Server** and the client computers are not joined in the same domain, you must check that the client computers have the option **Use simple file sharing** disabled (In Windows XP you can find it in "Control Panel -> Folder Option -> View -> Use Simple file sharing").

First Deployment Method: Computers Directory

The fastest way to deploy the agents is to go on the Unmanaged Computers node, under the Computers Directory:

1. *Right click* on an unmanaged computer (the ones with the gray icon) and select the "**Deploy on this computer**" option.

2. *Configure* the **agent deployment options**. Make sure the **server IP** is correct (it must be in the same network as the client computers).

3. Click **Start Deployment** to start the deployment process on the selected machines

Second Deployment Method: Network Builder

For Non Active Directory Situations use the following:

1. Via **Network Builder** on the dashboard, *choose* **Run Network Builder**, or via **Tools** *choose* **Network Builder**.

2. *Select* **Detected Network Computers.**

3. Within the **Computers Directory**, *right mouse click* on **Managed Computers** and *click* **Create New Group** e.g. Servers, Desktops, Sales.

4. If all computers are not being displayed, use "**ping range of computers to find them**" option.

5. Once created *drag and drop* the computers you wish to be placed within the newly created group.

6. *Click* **Apply changes.**

7. After the install (**Job Finished** will appear) click **Dismiss Page.**

8. The folder(s) will now appear within **Computers Directory \ Managed Computers \ New Folder** in the left hand pane, while the computers will appear in the right hand pane.

For Active Directory use the following:

1. Via **Network Builder** on the dashboard, *choose* **Run Network Builder**, or via **Tools** *choose* **Network Builder**.

2. *Select* **Active Directory Computers.**

3. If all computers are not being displayed, use "**ping range of computers to find them**" option.

4. *Drag and Drop* the **AD computer(s)** to the **Managed Computers group.**

5. *Click* **Apply changes.**

6. After the install (**Job Finished** will appear) click **Dismiss Page.**

7. The folder(s) will now appear within **Computers Directory \ Managed Computers \New Folder** in the left hand pane, while the computers will appear in the right hand pane.

Third Deployment Method: Deployment Tool utility

1. From the **Tools** menu *select* **Deployment Tool** option.

2. *Choose* what **type of installation** you want to do (you can select automatic install, or you can create an unattended package that you can later use to install the product on any computer). *Use* the "**Automatically Install**" option.

3. *Select* the product you want to install; in this case select the **BitDefender Management Agent** component.

4. *Choose* the **Install** option.

5. *Enter* the "**BitDefender Management Server Name or IP**" and the "**BitDefender Management Agent Port**" (use by default the server IP address, and the port selected in the Management Server installation – 7072 if you didn't changed the default options).

6. *Select* the **deployment options** (it's recommended to use the default settings).

7. If the client and the server are not in the same domain *use* the **Use non interactive Authentication** option, then *enter* the **computer\network credentials**, or *wait* for the **Deployment tool** to ask for them (after the deployment process start).

8. *Click* the **Next** button and then *select* the computers you want to deploy on.

9. *Click* the **Start** button to start the deployment process, and then *press* **Finish** after the deployment process has ended.

7.2.3.   Deploy/Install Client Products

The installation of the client products from the Management Server can be done using two methods.

- By using **Deployment Tool** and following the same steps as for installing the Agent;

- By applying a specific policy on a managed computer that has the **BitDefender Management Agent** installed on.

You can assign a policy using two methods:

- *Go to* **Create New Policy** section

- *Right Mouse click* on a **managed computer** or **group** and select the **Assign Policy** option

For each of the selected method you must follow the next steps:

1. *Select* the **Policy Template Category** (this is applicable to the type of group the policy is aimed for – you can select from **BitDefender Business Client**, **BitDefender for File Servers** or **BitDefender for Exchange** templates).

2. *Double click* on a policy to assign it.

3. *Configure* the settings.

4. *Click* **Finish.**

5. *Choose* and **Apply Schedule**

6. If you have created the policy from **Create New Policy** section you have to *select* the **target** from **Network computer** section (computer(s) or group(s) from **Computers Directory/server** also) or from **Network users and groups** section (user(s) or groups of user from **Active Directory**); if not, you won't see the target section.

8. *Click* on **Click Here to Assign this Policy** link.

9. For additional policies repeat from **Step 1** with the desired policy template.

7.2.4.   Install Server Products

To allow the deployment and management of the BitDefender for Windows Servers products from BitDefender Management Server you have to add the support files for BitDefender for Windows Server products in the BitDefender Management Server.

On the BitDefender Management Server machine, locate the BitDefender for Windows Servers Server Add-on setup file and double click it. This will launch a wizard, which will guide you through the setup process. If Management Server is installed on a 32-bit computer, you have to choose the 32-bit Server Add-on kit. If it is installed on a 64-bit machine, choose the 64-bit Server Add-on kit.

There are two ways to install the server products:

- **Using a centralized remote deployment through BitDefender Management Server.** Using BitDefender Management Server administration console you can deploy BitDefender Security for Windows Servers products on the wanted servers. The procedure is similar to the one for the Business Client product described at section 7.2.1.
- **Using a stand-alone local installation of the products.** You can install any BitDefender Security for Windows Server product by copying the BitDefender Security for Windows Servers setup file to the desired server and then selecting the products that you want to install. The intuitive wizard will guide you through the setup process. Then from the Management Console deploy the Management Agent on the server computers.

7.3.   Configuration and Important Settings

7.3.1.   Management Console

▪ BitDefender Management Server and its client products can be configured and managed through a graphical user interface named BitDefender Management Console.

▪ The new MMC-based management console was designed with the network administrator's needs in mind and focusing on improving user experience.

▪ To open the management console, use the Windows Start menu, by following the path: **Start→Programs→BitDefender Management Server→BitDefender Management Console.**

▪ Whenever you open the management console, you must provide the logon information of the BitDefender Management Server instance you want to connect to. To connect to BitDefender Management Server, fill in the following fields:

   ▪ **Management Server** - type in the IP address of the BitDefender Management Server instance you want to connect to.

   ▪ **Port** - type in the port used by the management console to communicate with the respective instance of BitDefender Management Server.

   ▪ **Username** - type in a valid username. The default username is administrator.

   ▪ **Password** - type in the password corresponding to the previously specified username. The default password is admin.

▪ When you connect to a BitDefender Management Server instance, its name and all of its objects will appear in the tree menu on the left, while the corresponding dashboard will be displayed on the right side of the management console window.

7.3.2.   Registration

▪ BitDefender Management Server comes with a trial period of 30 days. During the trial period, BitDefender Management Server can manage an unlimited number of BitDefender Business Client products.

▪ In order to register the selected instance of BitDefender Management Server, click Tools→Register.

▪ You can register BitDefender Management Server over the Internet or offline. If you want to register offline, you will need an authorization code (besides the purchased license key).

▪ To register BitDefender Management Server, follow these steps:

   1.   Select **Register this product**.

2.   Type the license key in the **Enter key** field.

3.   If you want to register the product offline, select **Perform offline registration** and type the authorization code in the **Authorization Code** field.

4.   Click **Finish**.

7.3.3.   Dashboard

- Each time you connect to an instance of BitDefender Management Server through the management console or click, in the tree menu, the name of such instance, a status pane is displayed. This status pane is referred to as the dashboard.

- The dashboard provides you with useful information on the status of the BitDefender Management Server instance and of its client products and it helps you easily solve the issues that require your attention. You should check the dashboard frequently in order to quickly identify and solve the issues affecting BitDefender Management Server or the network security.

- There are two or three status buttons at the top of the pane:

  - Management Server Status

  - Business Clients Status

  - Servers Status (if you have installed the Server Add-on)

- The status buttons change their colour depending on the existing issues.

  - **Green** status buttons indicate that no issue requires your attention.

  - **Yellow** status buttons indicate the existence of issues that pose medium security risks.

  - **Red** status buttons indicate the existence of issues that pose high security risks.

- The status buttons will turn to green when you fix the related issues, but they will go back to yellow or red whenever you forget to do important tasks or a new issue appears. For example, if you do not update BitDefender Business Client regularly, the Business Clients Status button will turn to red. In the same way, if you deploy BitDefender Management Agent on a computer without moving it into a specific group or you forget to change the default password, the Management Server Status button will turn to grey.

- Issues are displayed under the status buttons in a systematically organized list. Click a specific status button to see the related issues, if any.

- A yellow or red Management Server Status button indicates BitDefender Management Server-related issues that require your attention. Click the button to see the respective issues.

▪ Follow the instructions provided in order to fix the issues.

7.3.4. Computers Directory

▪ The Computers Directory tree in the console contains the network computers managed by BitDefender Management Server and other computers within the same subnet. BitDefender Management Server automatically detects all online network devices within the broadcast domain that have a configured network interface. Most of these detected devices are computers; however, management switches and router interfaces are also detected.

▪ The network computers are organized into three main groups:

  ▪ **Managed Computers** - contains the computers managed by BitDefender Management Server, namely those on which BitDefender Management Agent has already been installed. One or more BitDefender client products may also be installed on these computers.

  ▪ **Unmanaged Computers** - contains the detected network computers on which BitDefender Management Agent has not been deployed yet and which have not been excluded from the management scope of BitDefender Management Server. The first time you connect to a server, you will find all detected network computers in this group.

  ▪ **Excluded Computers** - contains the network computers which are not monitored at all by BitDefender Management Server. In this group you can find all network computers excluded from the Unmanaged Computers or from the Managed Computers group.

7.3.5. Policies

▪ BitDefender client products are administered remotely through policies. A policy defines a set of security rules a client computer must comply with.

▪ Policies are sent by BitDefender Management Server to BitDefender Management Agent, which applies them to the local BitDefender client product. Once a policy has been successfully transmitted to BitDefender Management Agent, it will be applied to the local BitDefender client product no matter if communication with BitDefender Management Server fails.

▪ Policies can be assigned to individual clients or to entire groups of clients.

▪ Every policy applied on a managed clients will check for the BitDefender Business Client installation status:

  ▪ If BitDefender Business Client is not present it will be installed first and only then the configured policies will be applied

  ▪ If the BitDefender Business Client is present, the configured policies will be applied immediately

- Policies can be configured and applied based on the templates the solution provides. To create a policy:

    1. Go to node **Policies/Create New Policy** and select one of the categories provided (in this case, Business Client).

    2. Configure the policy by editing the template settings. Click Finish

    3. Select the computer, group or domain user to assign the policy to.

    4. Select the schedule according to which the policy should run.

    5. Click the provided link to assign the policy. The new policy will appear in the Current Policies pane

- To check whether the set policy has been applied to the target machine/s, go to the **Current Policies** node, select the item you are interested in and right click it. In this way, you will get access to the **"More details"** option, which will indicate the actual machines the policy in question has been applied on.

- To make sure the policy has been successfully applied on all intended stations, open the dashboard page and check whether there have been any errors.

7.3.5.1.   Exporting and Importing Policies

- If you use several BitDefender Management Server instances to manage the network, you do not have to configure the security policies separately for each of them. Once you have configured all the necessary policies on a particular BitDefender Management Server instance, you can use **Tools→Export/Import Policies** to replicate policies on the other BitDefender Management Server instances.

- The policy replication process consists of these main steps:

    1. Export current policies configured on a specific BitDefender Management Server instance to a policies file.

    2. Transfer the policies file to the BitDefender Management Server computers on which you want to replicate the saved policies. You can also copy the policies file to a network share available to these computers.

    3. Import the policies from the policies file to the other BitDefender Management Server instances.

    4. Assign the imported policies to managed computers and groups, as needed.

7.3.6.   WMI Tasks

- Aside from the policy templates, which are the main element of the solution, BitDefender Management Server also comes with a series of useful WMI-based scripts that integrate with the BitDefender policy technology in order to facilitate

administrative control over the network. You can run these WMI scripts on the remote network computers managed by BitDefender Management Server, in order to:

- find out useful information about the network computers, such as system information, installed software, startup programs, free disk space and so on.
- remove software installed on the network computers.
- kill specific processes running on the network computers.
- restart or shut down the network computers.
- log off the user logged on to the network computers.

- The application of WMI scripts is similar to that of policies. WMI scripts can be configured and applied based on the templates provided in the solution. To access these templates, go to node **WMI scripts** /**Create New WMI scripts** and select one of the categories provided. A WMI script template allows creating a script that you can assign to managed computers in order to find out useful information about them or perform a specific administrative task.

7.3.7.   User Control

The User Control functionality can block access to:

- Inappropriate web pages.
- The Internet, for certain periods of time (such as during the working hours).
- Web pages and e-mail messages if they contain certain keywords.
- Applications like games, chat, file sharing programs or others.

7.3.8.   Privacy Control

- BitDefender monitors dozens of potential "hotspots" in your system where spyware might act, and also checks any changes made to your system and software. It is effective in blocking Trojan horses and other tools installed by hackers, who try to compromise your privacy and send their personal information, like credit card numbers, from your computer to the hacker. BitDefender also scans the web sites that you visit and alerts you if any phishing threat is detected.

- The Privacy Control protects your computer using these important protection controls:

    - **Identity Control** - protects your confidential data by filtering all outgoing HTTP and SMTP traffic according to the rules you create in the Identity section.

- **Registry Control** - asks for your permission whenever a program tries to modify a registry entry in order to be executed at Windows start-up.

- **Cookie Control** - asks for your permission whenever a new website tries to set a cookie.

- **Script Control** - asks for your permission whenever a website tries to activate a script or other active content.

7.3.9. Reports

- Reporting Center allows you to create centralized reports on the computers managed by BitDefender Management Server, which you can use to find out:

  - Information about the malware activity on all managed computers.

  - The status of the BitDefender client products.

  - Which BitDefender client products are not up to date.

  - What software is installed on the managed computers.

- Reports are created using the Crystal Reports technology, based on report templates and on the information existing in the BitDefender Management Server's database. They provide you with:

  - Statistical data regarding all managed computers.

  - Detailed information for each managed computer or BitDefender client product.

- You can create and manage reports in the Create New Report pane. To display this pane, do one of the following:

  - In the tree menu, go to **Reporting Center > Create New Report**.

  - In the Reporting Center pane, click the link provided.

- You can see the report templates that you can use to create reports. To create a report, follow these steps:

  - Right-click the report you want to create and select "**Create report**". A new pane will be displayed.

  - Select the BitDefender Management Server instance to create the report for.

  - For malware activity reports, specify the time interval to be covered in the report.

  - Click the provided link in order to create the report.

- The reports created are displayed in the **Create New Report** pane. At the top of the first report page, you can see the report name, date and, for malware activity reports, the period it covers. The first page provides you with statistical data (pie

charts and graphics) for all network computers managed by BitDefender Management Server. There follows detailed information on each managed computer. The reports created are not automatically saved on the disk. To save the information they contain, you can export reports or print them.

7.3.10. E-mail alerts

- BitDefender Management Server can notify you through e-mail about important issues affecting the network security. The e-mail notifications may help you block threats to the network security in a timely manner.

- If you configure e-mail notifications, BitDefender Management Server will check for the selected security issues regularly, based on the configured checking interval. If new security issues have occurred since the last check, you will receive an e-mail with the cumulative issues occurred since the last alert was received.

- In order to receive e-mail notifications, you must first configure the e-mail settings. Click **Tools→E-mail Settings** on the menu.

     1.   To specify for which issues to receive e-mail notifications, follow these steps:

     2.   In the tree menu, click the BitDefender Management Server name to display the dashboard.

     3.   Follow the link to configure the dashboard.

     4.   Select the check boxes from the Send e-mail alerts column corresponding to the issues that you want to be notified about through e-mail.

     5.   Click OK to save the changes.

7.3.11. Backup and Restore Server Configuration

- Backup/Restore Server Configuration Tool helps you save the BitDefender Management Server configuration to a backup file or restore a previously saved configuration of BitDefender Management Server. This tool is very useful in the following situations:

     - Moving BitDefender Management Server to another machine.

     - If the BitDefender Management Server configuration is corrupted.

     - Reinstalling the operating system.

     - Reinstalling BitDefender Management Server.

- BitDefender Backup/Restore Configuration tool can be accessed from the Management Console, Tools→Backup/Restore Configuration. An intuitive wizard will guide you through the steps to perform the operation.

8. BitDefender Awards and Certifications

BitDefender solutions consistently earn top marks from independent testing organizations and are recognized by top industry publications.

9. Contact Info

Main site:	www.bitdefender.com
Sales department:	sales@bitdefender.com
On-line Store	www.bitdefender.com/site/Buy/products/
Find a distributor:	www.bitdefender.com/site/Partnership/list/
Technical support:	b2b@bitdefender.com
	http://kb.bitdefender.com