

BitDefender for File Servers

Technical Whitepaper





1. Introduction

Nowadays file servers, along with the e-mail, are the main data management tools. Storing, sharing and distributing data are the main data management tasks and they would fail without easy access to information, data integrity and good system uptime. The file server is one of the most vulnerable network resources. If infected or brought down, it could make all the other network resources unavailable. One infected file could determine the infection of a large amount of data, loss of data integrity and eventually render the system inoperative. The risks involved result in high costs for network and file server management.

BitDefender for File Servers addresses the issues of data security and system availability with:

- **Economic benefits**
 - Increased productivity due to maximized system uptime and data availability
 - Lower risk of data loss due to the antivirus protection offered by BitDefender
 - Less money invested in network maintenance and training
 - Additional security and compliance with security standards and laws
- **Technical benefits**
 - High performance, low impact and maximized uptime
 - Minimum resource use
 - Fastest response time and certified antivirus engines
 - Easy to use and implement
- **BitDefender advanced technologies**



2. Features

BitDefender for File Servers is a solution especially implemented for servers running on the Windows platform. Its main features cover the security needs of a file sharing server, while its purpose is to lower the burden implied by administrating a server software solution. Easy to install and easy to configure, but with a strong set of functionalities, it targets both small and large organizations.

Feature	Benefit & Description
B-HAVE	<p>Protects company data against unknown viruses (that do not have a signature), thus preventing data loss, system instability and other damages that could affect the business.</p> <p>B-HAVE stands for Behavioral Heuristic Analyzer in Virtual Environments; practically, it emulates a virtual computer-inside-a-computer where pieces of software are run in order to be checked for potentially malicious behavior. This BitDefender proprietary technology represents a new security layer that keeps the operating system safe from unknown viruses by detecting potentially malignant pieces of code for which signatures have not been released yet. It thus supplements usual signature and behavior-based techniques, increasing the overall effectiveness of your antivirus solution. B-HAVE is a component of the BitDefender antivirus engines, which have been certified by ICSA Labs, CheckMark, CheckVir, Virus Bulletin and TUV.</p>
Scan Optimization	<p>Saves system resources using optimized scanning methods.</p> <p>The BitDefender antivirus scanner fingerprints every scanned “read-only” file, during each session. The “read-only” permission ensures that the file will not be modified or infected during the respective session. A database of recently scanned files that have been found to be safe is thus created. These files are not rescanned upon a new access. If an update is performed or if an infection is detected in the system, the database is reinitialized. This safety measure ensures that all files are rescanned with the latest antivirus signatures.</p>
Multithread Scanning	<p>Reduces the time spent on the scanning process.</p> <p>Multithread scanning implements a well-known method that simulates the parallel execution of a program.</p>



Feature	Benefit & Description
On-access Scanner	<p>Multiple instances of the engines are used in order to shorten the scanning process.</p> <p>Protects the company's data against known malware, in real-time, thus preventing data loss, system instability and other damage that could affect the business.</p>
On-demand Scanner	<p>On-access scanning provides real time protection of the file server by scanning every file that is accessed or copied on the disk. This is the main feature of a server-oriented antivirus application and its function is to keep the file server free from malicious content.</p> <p>An additional feature which ensures the safety of the company data.</p> <p>On-demand scanning is a powerful tool specially designed for administrators. Its purpose is to provide a second layer of defense against malicious software that might infect the file server. We recommend that you scan the file server periodically with the newest antivirus signatures by scheduling an on-demand antivirus scan or by performing a scan-now action.</p>
Threat Mitigation	<p>Provides fast response time against the latest threats.</p> <p>Automated signature and product updates, backed up by the B-HAVE technology, minimize the window of vulnerability of your system. The updates are automatically downloaded from BitDefender servers or approved mirror sites hourly.</p>
Scheduler	<p>Increases data availability by reducing the interference of the product activity with the work schedule.</p> <p>Scheduling capabilities have been added to BitDefender for File Servers. On-demand antivirus scans and update tasks can be scheduled from the product user interface. This system has been correlated with the Alerts module to provide notifications for administrators when an on-demand scan or an update has been performed.</p>
Logging and Statistics	<p>Improves server monitoring and reduces the time spent on creating reports and statistics regarding product activity.</p> <p>The monitoring system has been improved as well. Reports of the product activity can be created and a special statistics module is provided. Also, the alert</p>



Feature	Benefit & Description
<p>Redesigned Interface</p>	<p>system includes new features as customizable alerts for several types of events: antivirus signature updates, product updates, on-demand scans, viruses detected.</p> <p>Reduces costs and the time spent on training system administrators.</p> <p>BitDefender for File Servers has an MMC-based user interface that offers a friendly working environment. The wizard system implemented in the interface enhances the usability of the product while the snap-in system provides the actual management functionality.</p>
<p>Centralized Management</p>	<p>Saves time and money spent on network maintenance.</p> <p>BitDefender for File Servers is fully compatible with BitDefender Enterprise Manager, offering organizations a centralized type of management for antivirus protection and security policies inside complex networks. It is possible to remotely install, configure and check the status of BitDefender for File Servers in a centralized manner, from an administrative console in your network.</p>
<p>24/7 Support</p>	<p>Free and prompt professional assistance for any issue or question you might have regarding the product.</p> <p>Offered online by qualified support representatives and an online database with answers to Frequently Asked Questions.</p>



3. Architecture

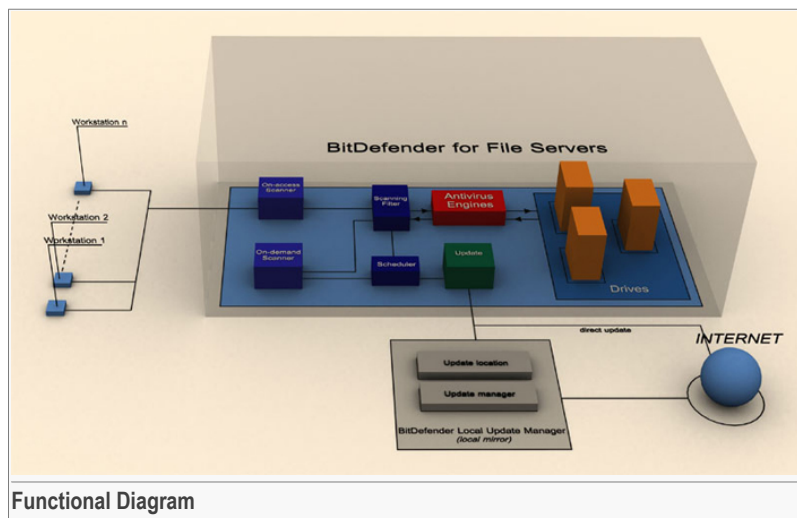
BitDefender for File Servers was designed with the following attributes in mind:

- high usability;
- logical, efficient and thorough working mechanism.

Therefore, the product comes with an easy-to-use interface that has a modular structure. However, these modules do not necessarily correspond to the internal product architecture.

3.1. Functional Diagram for End-Users

The diagram below shows how BitDefender works.



Functional Diagram

To better serve its function as a security solution meant for servers, **BitDefender for File Servers** is based on a modular architecture. These are its main modules:

- **On-access Scanner**
- **On-demand Scanner**
- **Update**
- **Scheduler**
- **Content Filter**
- **Antivirus Engines**



Real-time Protection. As the files are being written on the disk or accessed, the On-access Scanner module intercepts the event and starts the scanning process.

The scanning process comprises the following steps:

1. The content filter checks the file. The file extension, the file size, the file path are sequentially checked to match the administrator configurations. The result of the Content filtering process is SCAN or NO SCAN.
2. If the result of the Content Filter is SCAN, the file is scanned by the Antivirus Engines. First the file is checked against the antivirus signatures database. If any part of the file matches a signature, the file is reported as infected. If none of the signatures is matched, the file is checked with the B-HAVE technology. In case the behavior of the file is similar to the behavior of a piece of malware, it is reported as infected. The result of the Antivirus engines module can be INFECTED or CLEAN.
3. If the file having passed through the Antivirus Engines module is INFECTED, one of the following actions can be taken: disinfect, delete, ignore, quarantine. If these actions fail, the **Deny access** action is applied so that the user will not be able to execute the infected code.

On-demand Scanning. The On-demand Scanner can be triggered by clicking **Scan now** from the user interface or by a scheduled on-demand scan task. This scanning process is similar to the real-time protection scanning. The difference is that the on-demand scanning will not apply to the accessed files, but to those submitted by the user to this purpose.

Update. The Update module performs the update process and its main function is to download the latest BitDefender files. Three types of files are available:

- **Antivirus signatures** - These files are updated constantly as the BitDefender Lab analyzes new viruses every day.
- **Antivirus engines** - These files are updated as frequently as the antivirus signatures B-HAVE, a BitDefender proprietary technology, has been implemented in the antivirus engines.
- **Product files** - The product file updates differ from the antivirus signature updates and their function is to deliver bug fixes and performance improvements brought to the product. Product updates are downloaded, but they are not automatically installed. Please note that the installation of product updates might require a system restart.

Note



The update process is performed automatically every, 3 hours, but the time interval can be configured and the update tasks be scheduled at any time.

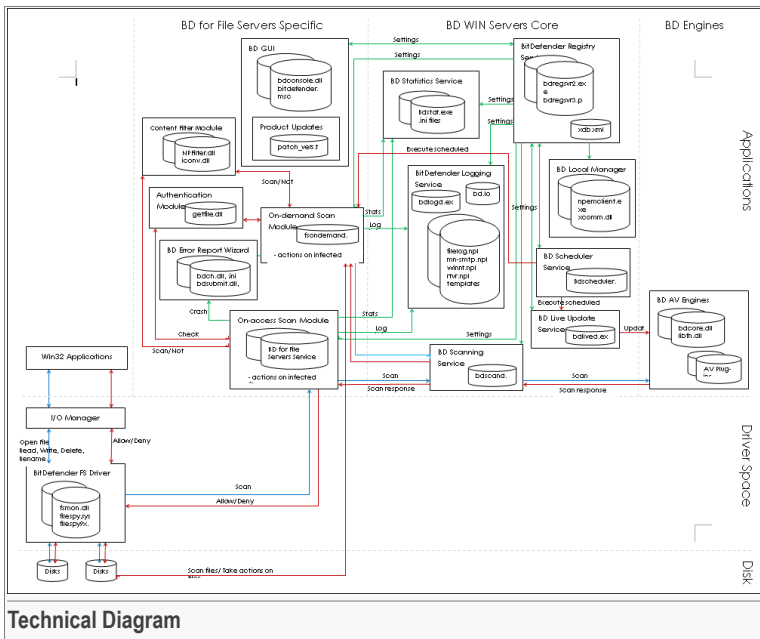
The download of the latest BitDefender files requires an approved BitDefender update location. By default, the product updates the files from the BitDefender sites, but local



mirrors of the BitDefender update locations can be made by installing BitDefender Local Update Manager. The installation kit for the **BitDefender for File Servers** also includes the BitDefender Local Update Manager. In this way, the **BitDefender for File Servers** products can be updated from a location within the same network.

3.2. Technical Diagram - In-depth View

The previous diagram presented the basic functionality of BitDefender from the end user perspective. This section aims to present the BitDefender in-depth working mechanism.



Technical Diagram

BitDefender Components

This is a list of the BitDefender components, together with an explanation of the purpose they serve:

BitDefender Registry Service

The **BitDefender Registry Service** manages the BitDefender settings. It receives requests from the BitDefender components to read data from or to write data into the



settings file. For example, when a component is registered, it sends its default settings to the BitDefender Registry Service, which writes them in the `xdb.xml` file. Therefore, all BitDefender components depend on this service.

BitDefender Scanning Service

This service is in charge of the scanning process. It receives from the On-access and On-demand scan modules the files to be scanned and it scans them using the antivirus engines and plugins.

BitDefender Antivirus Engines

The BitDefender Antivirus Engines and the Antivirus Plugins are loaded by the BitDefender Scanning Service when scanning files.

Content Filter Module

Decides whether the file should be scanned or not based on the settings specified by the user in the console (or on the default settings).

Authentication Module

Connects to the key server and checks if the license key is valid or not. If not, the product qualifies as unregistered and the scanning process will be cancelled.

BitDefender File Server Driver

It is a kernel level module that detects when the files on the disk are accessed (open, read, write, rename, delete). The files are sent for scanning to the On-access Scan module, which indicates in reply the action to be taken: **Allow / Deny access**.

On-access Scan Module (BitDefender for File Server Service)

Ensures that accessed files are scanned.

It receives the accessed file from the BitDefender driver and sends it to the Content Filter to see if it should be scanned or not. If the Content Filter response is SCAN, it will send the file to the Scanning Service to be scanned. Based on the scan result, an appropriate action will be taken by the service and the **Allow / Deny access** response will be sent to the driver.

BitDefender Error Report Wizard

If the BitDefender processes (services and on-demand scanning) encounter errors during their execution, a dump file is created and a wizard is opened in order to submit a report to the BitDefender Lab.



Console

The BitDefender Console is the graphical user interface (GUI), which allows the user to change product settings, take actions and monitor the file server.

On-demand Scan Module

Sends the files indicated in the interface by the user to the Content Filter Module to see if they should be scanned or not. If the Content Filter response is SCAN, it will send the files to the Scanning Service. Based on the scan result, an appropriate action will be taken.

BitDefender Logging Service

Receives the information sent by the agent components (the On-access and On-demand Scan modules) and manages it using four plugins:

- **filelog.npl** - logs the information in the log file. Its location is stored in the `BDUX/LoggerDaemon/Plugins/Filelog/Location/` key from the BitDefender registry (`xdb.xml`).



Note

The default log file is: `C:\Program Files\Common Files\Softwin\BDLog\bd.log`.

- **mn-smtp.npl** - sends mail alerts to the specified receivers.
- **winnt.npl** - sends net send alerts to the specified receivers.
- **rtvr.npl** - sends reports to the BitDefender Lab regarding the real-time virus activity on the local machine.



Important

The settings regarding the BitDefender Logger can be seen and modified in the `BDUX/LoggerDaemon` key from the BitDefender registry (`xdb.xml`).

BitDefender Statistics Service

Manages the BitDefender statistics.

BitDefender processes (usually the On-access and On-demand Scan modules) send statistics information to the service. Based on this information, it generates statistics and reports when requested by the console or the Scheduler Service (through a scheduled task).

BitDefender Live Update Service

Keeps BitDefender up to date by searching for updates on a regular basis.

**Note**

For more information about this service and the corresponding module from the user interface, check [“Update.”](#) (p. 7).

BitDefender Scheduler Service

Schedules on-demand scan and update tasks to be executed at a later time (periodically or one-time only).

Workflows

- **How the on-access scanning process works.**

These are the stages of the on-access scanning process:

1. As a file is being written on the disk or accessed, the BitDefender File Server Driver intercepts the event and informs the BitDefender for File Servers Service, waiting for a response.
2. The BitDefender for File Servers Service sends a request to the Content Filter to see if the file must be scanned or not.
3. The Content Filter checks the file. The file extension, the file size, the file path are sequentially checked to match the administrator configurations. The result of the Content filtering process is SCAN or NO SCAN.
4. If the result received from the Content Filter is SCAN, the file is sent to the BitDefender Scanning Service for analysis. If not, an **Allow access** response will be sent back to the BitDefender Driver and no action will be taken on the event (the operation will be allowed).
5. The BitDefender Scanning Service loads the antivirus engines and plugins and scans the file. First, the file is checked against the antivirus signatures database. If any part of the file matches a signature, the file is reported as infected. If none of the signatures matches, the file is checked with the B-HAVE technology. In case the behavior of the file is similar to that of a piece of malware, it will be reported as suspect. The Scanning Service can decide that the file is INFECTED, SUSPECT or CLEAN.
6. If the scan result is INFECTED or SUSPECT, the BitDefender for File Servers Service takes the appropriate action on the file, based on the settings from the BitDefender Registry. The result is also communicated to the BitDefender Driver, which denies access to the infected file. Otherwise, an **Allow access** response will be sent to the BitDefender Driver and no action will be taken on the event (the operation will be allowed).
7. At the end of the scanning process, all scan-related information is then sent to the BitDefender Logger and Statistics services which manage it accordingly.

The BitDefender for File Servers Service communicates with the **Authentication Module** once a day to check the validity of the product. If the key has expired or if



it is found invalid (a key can be invalidated from the key server) the product is unregistered and the on-access protection is disabled.

If an error occurs during the scanning process, the BitDefender Error Report Wizard takes over in order to send the error report to the BitDefender Lab.

- **How the on-demand scanning process works.**

The on-demand scanning process scans files when the user or a scheduled scan request it. The scan settings are the same as those of the on-access scanning module. The main difference is that with on-demand scanning, only the files the user specifies in the management console are scanned.

After specifying the scan settings and the files to be scanned in the console, the user triggers the scanning process by clicking the **Scan now** button. The process can also be initiated through the BitDefender Scheduler Service by creating a scheduled scan task.

The scanning parameters are sent to the BitDefender Registry. The On-Demand Scan module sends a request to the BitDefender Registry Service to receive these settings and initiates the scanning process.

First, an authentication request is sent to the **Authentication Module** to check the validity of the product. If the key has expired or if it is found invalid (a key can be invalidated from the key server) the product is unregistered and the scan process is cancelled. If the product is valid, the Content Filter is called to see which files to scan.

Further on, the process is identical to the on-access scanning, except no communication with the BitDefender Driver is involved. A scan report can be generated.

- **How the update process works.**

The update process is performed by the BitDefender Live Update Service. This service automatically checks for available updates, based on the settings specified in the xml settings database:

- **update location** - an update server or a local mirror in the network.
- **connection type** - the service can connect to the Internet directly or through a proxy server. The proxy settings can also be found in a registry key in `xdb.xml`.
- **time interval** - the time interval between two consecutive searches. The service computes the time interval since the last check (which can also be found in `xdb.xml`) and decides when to check for updates next.

The update procedure is different, depending on the type of update:

- **antivirus engine / signatures update** - if available, the update files are downloaded to the disk. After the download is finished, the old files are replaced with the new files.



- **product update** - if the update is a new patch, then it is downloaded to the disk and the user is informed through the management console about it. If a new kit is available, the user is informed through the management console about its version and location.

The update process can also be triggered by the user (by clicking the **Update now** button from the management console) or by a scheduled update task.

- **How the user interacts with the product.**

The user interacts with the product through the management console: he or she specifies settings, monitors the product activity, commands certain tasks. Any change made in the management console is sent to the BitDefender Registry Service, which modifies the corresponding key from the xml settings database accordingly.

The settings are sent to the product components by the BitDefender Registry Service **only** as a result of their request. Each component decides when to send such a request to the service. Usually, this request is in their message waiting queue or in the main cycle of each module.

- **How the scheduling works.**

Through the management console, the user configures scheduled update and scan tasks. The settings are transmitted to the BitDefender Registry Service, which writes the appropriate keys in the database and sends them to the BitDefender Scheduler Service, upon request.

The BitDefender Scheduler Service uses these settings to indicate when an update or scan process must be performed. It computes when the task must be launched and sends the appropriate request to the Scanning or to the Update Service

- **How it integrates with BitDefender Enterprise Manager.**

The installation kit comes with the `npemclient.exe` file and the files for the additional task templates. The `npemclient.exe` file is the one that integrates BitDefender for File Servers with the BitDefender Enterprise Manager. Initially, this file is not installed, and the two products integrate only after BitDefender Local Manager is deployed on the local machine, when several other files are copied.

The BitDefender Local Manager interacts with the product as follows:

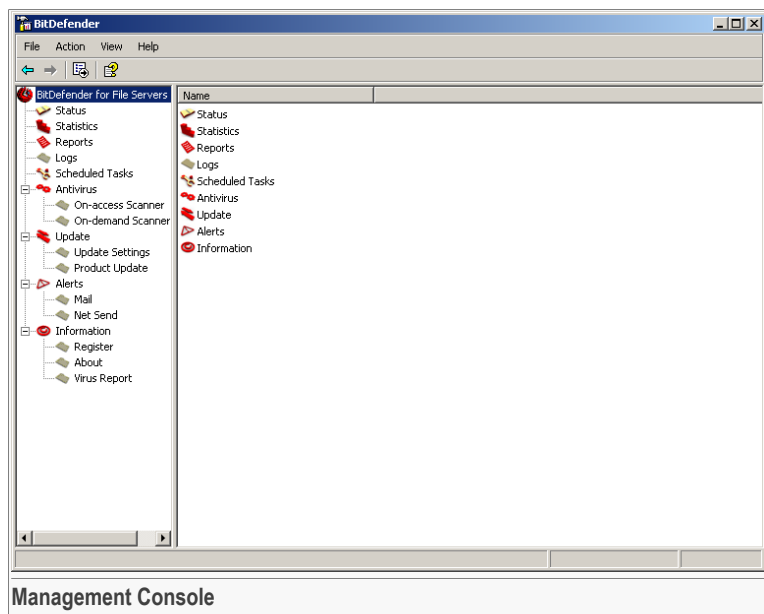
- to configure the product, BitDefender Local Manager sends a request to the BitDefender Registry Service to write in `xdb.xml`;
- to get status or statistics information, BitDefender Local Manager sends a request to the BitDefender Registry Service to read from the BitDefender registry and send back the required data;
- to scan or update the product, BitDefender Local Manager communicates with the Scanning or Update Service, through BitDefender Registry Service, which then initiates the respective process.



4. User Interface

BitDefender for File Servers was designed with an MMC based interface, which allows for all of the protection options of all BitDefender modules to be configured.

To open the management console, access the Windows Start menu and follow this path: **Start** → **Programs** → **BitDefender for File Servers** → **BitDefender for File Servers** or quicker, double click the **BitDefender** icon from the system tray.



4.1. BitDefender Modules

On the left side of the management console there is the module selector. In order to make BitDefender easier to use, the BitDefender modules have been organized into three categories:

- **Monitoring** - includes the modules: **Status**, **Statistics**, **Reports** and **Logs**. These modules provide information on the product activity and status and they help monitor the file server. Given their role, these modules require frequent access.



- **Configuration** - includes the modules: **Scheduled Tasks**, **Antivirus**, **Update** and **Alerts**. These are the configuration modules, which require your attention at the end of the installation and every now and then.
- **General** - includes the **Information** module. The module needs to be accessed at the end of the installation in order to register the product and, optionally, to configure the RTVR. Later on, it won't be necessary to access this module unless the license key needs to be changed.

Here is a description of each module:

- **Status** - provides essential information about the product (antivirus and update status).
- **Statistics** - offers statistics regarding the antivirus activity based on the BitDefender log file and other such resources.
- **Reports** - allows creating customized report files based on the BitDefender log file and other such resources.
- **Logs** - offers quick access to the last BitDefender log file. The BitDefender log file contains valuable information regarding the product activity (viruses found, update processes and on-demand scheduled scan tasks performed, product errors, registration details).
- **Scheduled Tasks** - allows creating scheduled tasks for both the update and the scanning processes through an intuitive wizard. The scheduled tasks allow updating BitDefender or scanning the file server when the machine is idle, so as not to interfere with the usual activities or waste system resources.
- **Antivirus** - helps configure the **On-access Scanner** and the **On-demand Scanner**. The **On-access Scanner** prevents new viruses from entering the system, thus providing with real-time protection. The **On-demand Scanner** detects viruses that already reside in your system, by scanning all or part of such system, upon request.
- **Update** - helps configure the **Update** module in order to get the latest updates (in the **Update Settings** section) and informs you whether product updates or upgrades are available (in the **Product Update** section).
- **Alerts** - allows configuring BitDefender so as to send alert messages (by e-mail or through netsend) to the people in charge with network security, under special circumstances (when a virus is found, when an error occurs, after a scheduled on-demand scan is completed or when the product is about to expire).
- **Information** - contains general settings and information regarding BitDefender. Here you can register the product (in the **Register** section), see product details (in the **About** section) and configure the RTVR (in the **Virus Report** section).

At the bottom of the management console information is available on the section you are into.



4.2. Remotely Connecting to Another Computer

BitDefender allows remotely connecting to another computer that has **BitDefender for File Servers** installed. This management capability helps organizations reduce costs, by providing a minimal centralized administration of all the products installed on the company servers.



Important

When remotely connecting to another computer on which **BitDefender for File Servers** is installed, you will not have access to all the product features, but you will be able to perform an **update by user request** and to enable/disable the **On-access scanner**.

In order to be able to connect remotely to another computer, you need to:

1. **Specify a password for the target server.** Open the management console on the target server. Right-click **BitDefender for File Servers** from the module selector, select **Change administrative password** and, in the window that opens, specify the password.
2. **Connect to the target server.** Open the management console on your server. Right-click **BitDefender for File Servers** from the module selector, select **Connect to another computer** and, in the window that opens, specify the server IP and the password.

To find out more about the management console (user interface), please check the **Management Console** part of the product's **User's Guide**.



5. Installation and Configuration

5.1. System Requirements

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

- **Minimum Processor** - Pentium II 300 MHz
- **Minimum hard disk space** - 75MB
- **Minimum RAM Memory** - 64MB (128MB Recommended)
- **Operating platform** - Windows NT 4.0 SP6 + Internet Explorer 5.5 + MMC v1.2 / Windows 2000 / Windows XP or Windows 2003 Server

5.2. Install BitDefender for File Servers

There are two ways to install **BitDefender for File Servers**:

- **automatically**: using the installation kit, you need to complete a setup wizard.
- **manually**: using the product files, you need to copy, register and install each file and service manually.

Each method is described further.

Automatic Installation

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 with these terms click **Cancel**. The installation process will be abandoned and you will exit setup.
3. A new window containing a list of all BitDefender components will appear. Select the ones you would like to install.

If you click any component name, a short description (including the minimum space required on the hard disk) will appear on the right side. If you click any component icon, a window will appear where you can choose whether to install the selected module or not.

Click **Next**.

4. Click **Next**.



5. The readme file contains important notes regarding **BitDefender for File Servers**. To open it at the end of the installation select the check box corresponding to **View Readme file**.
Click **Install** in order to begin product installation.
6. Click **Finish** to complete product installation.

Manual Installation

BitDefender for File Servers can also be installed manually, if the product files are available.

The installation kit is an executable archive which contains a `.msi` file and other files needed for installation. The `.msi` contains a `.cab` archive, which stores all of the product files.

Prerequisites. Before installing the product, you need to:

1. Get the product files (from developers or testers, from the kit by unpacking it, then the `.msi`, and finally the `.cab` or by other means).
2. Copy each file to the location where it would normally be installed.

You can change the location of the files that are normally installed in `\Program Files\Softwin\BitDefender for File Servers`, but keeping the subdirectory structure. The files from `\Program files\Common Files\Softwin`, however, must be copied in the same place.

To find out more about the installation folders and most important files, check the [File List](#) section of this document. To get the complete list of files and folders, check "[Appendix B - File List](#)" (p. 63).

3. Enter a command line interface (shell) in order to register / install all the necessary services and files.



Important

When you register / install a file make sure that the current directory in the shell is the one where the file is located.

Begin installation. To actually install the product, you must register / install some BitDefender components (mainly services). The procedure for each of them is described further. We recommend that you observe the following order:

BitDefender Registry Service

Default path: `\Program Files\Common Files\Softwin\BDReg\bdregsvr2.exe`.

Currently, there is no command to install or start this service due to a bug in the product. Find an appropriate tool in order to do it.

**Important**

This service must be running in order to register / install the other BitDefender components.

BitDefender Scanning Service

Default path: `\Program Files\Common Files\Softwin\bdscand.exe`.

To install and start this service, enter the following commands in the shell:

1. **bdscand register** - register the service in the BitDefender registry.
2. **bdscand install** - register the application as a Windows service.
3. **bdscand start** - start the service.

BitDefender Logging Service

Default path: `\Program Files\Common Files\Softwin\bdlogd.exe`.

The BitDefender Logging Service manages and logs the information sent by agents using four plugins: `filelog.npl`, `mn-smtp.npl`, `winnt.npl` and `rtvr.npl`. These plugins are located by default in: `\Program files\Common Files\Softwin\BDLog`.

To install and start this service, enter the following commands in the shell:

1. **bdlogd register** - register the service in the BitDefender registry.
2. **bdsetup install "filelog.npl full path" "filelog.npl installation path"** - install the plugin. You must specify the path to the file (full or relative) and the full installation path.

Note

Example: **bdsetup install "/BDLog/filelog.npl" "C:\Program Files\Common Files\Softwin\BDLog"**

3. **bdsetup install "mn_smtp.npl full path" "mn_smtp.npl installation path"** - install the plugin. You must specify the path to the file (full or relative) and the full installation path.

Note

Example: **bdsetup install "/BDLog/mn_smtp.npl" "C:\Program Files\Common Files\Softwin\BDLog"**

4. **bdsetup -i "nn-winnt.npl installation path"** - install the plugin. You must specify the full installation path.

Note

Example: **bdsetup -i "C:\Program Files\Common Files\Softwin\BDLog"**



5. **bdsetup install "rtvr.npl full path" "rtvr.npl installation path"** - install the plugin. You must specify the path to the file (full or relative) and the full installation path.

Note

Example: **bdsetup install "/BDLog/rtvr.npl" "C:\Program Files\Common Files\Softwin\BDLog"**

6. **bdlogd install** - register the application as a Windows service.
7. **bdlogd start** - start the service.

BitDefender Statistics Service

Default path: `\Program Files\Common Files\Softwin\Stats\BDStat.exe`.

To install and start this service, enter the following commands in the shell:

1. **BDStat /install** - register the application as a Windows service.
2. **BDStat /start** - start the service.

BitDefender Live Update Service

Default path: `\Program Files\Common Files\Softwin\bdlived.exe`.

To install and start this service, enter the following commands in the shell:

1. **bdlived register** - register the service in the BitDefender registry.
2. **bdlived install** - register the application as a Windows service.

BitDefender for File Servers Service

Default path: `\Program Files\Softwin\BitDefender for File Servers\bdfs.exe`.

To install and start this service, enter the following commands in the shell:

1. **bdfs /register** - register the service in the BitDefender registry.
2. **bdfs /install** - register the application as a Windows service.
3. **bdfs /start** - start the service.

BitDefender Console

Default path: `\Program Files\Common Files\Softwin\Console\bdconsole.dll`.

To register the BitDefender Console use the following command: **regsvr32 bdconsole.dll**.

On-Demand Scan Module

Default path: `\Program Files\Softwin\BitDefender for File Servers\fsdemand.exe`.

To register the On-Demand Scan Module use the following command: **fsdemand register**.



5.3. Configure BitDefender

In order to ensure a virus-free file server follow these steps:

1. **Register the product.** Access the **Information** module, **Register** section and click **Register BitDefender for File Servers**. In the window that opens, enter the license key and click **Apply&OK**.
2. **Activate your Support Account.** In order to benefit from free technical support and other free BitDefender services, access the **Register** section (**Information** module) and click **Online Registration** in the BitDefender Help menu.
3. **Apply available Product Updates.** Access the **Update** module, **Product Update** section, and install the product updates, if any.
4. **Configure the update.** Access the **Update** module, **Update Settings** section and click **Configure BitDefender Update**. In the window that opens, set the update interval and the update location and click **Apply**. Click **Scan now** to make sure you have the latest virus signatures.



Note

If you do not want the update process to interfere with the server activity you have the possibility to schedule the update process. Access the **Scheduled Tasks** module, right-click this section and select **New task**. Complete the wizard that appears, configuring the appropriate settings, in order to create a scheduled update task.

5. **Configure BitDefender alerts.** If a virus is detected or an unexpected situation appears, it is possible for alarm messages to be sent by e-mail or by net send. Access the **Alerts** module and configure BitDefender to send these notifications.
6. **Check product compatibilities.** Exclude folders from both on-access and on-demand scanning as recommended in the [“Exclude Folders from Scanning”](#) (p. 23) section of this user guide.
7. **Configure the On-access Scanner.** Access the **Antivirus** module and configure the **On-access Scanner**.
8. **Test your BitDefender.** Test you antivirus product as described in the [“Check if BitDefender is Working”](#) (p. 23) section of this user guide.
9. **Configure the On-demand Scanner.** Access the **Antivirus** module and configure the **On-demand Scanner**. Also, perform a full on-demand scan: click the **Scan now** button from the configuration window.
10. **Create a scheduled scan event.** We recommend that you scan the server at least once a week. If you do not want the scanning process to interfere with the server's activity you have the possibility to schedule the scanning process. Access the **Scheduled Tasks** module, right-click it and select **New task**. Complete the wizard that appears, configuring the appropriate settings, in order to create a scheduled scan task.



To find out more about configuring the product, please check the product's **User's Guide**.

5.4. Check if BitDefender is Working

The file can be created using any text editor, provided the file is saved in standard MS-DOS ASCII format and is 68 bytes long. It might also be 70 bytes if the editor puts a CR/LF at the end.

The file must contain the following single line:

Copy this line and save the file with any name and `.COM` extension, for example `EICAR.COM`. BitDefender must treat this file as an infected one.

There is no reason to worry, because this file is not a real virus. All that `EICAR.COM` does when executed is display the text `EICAR-STANDARD-ANTIVIRUS-TEST-FILE` and exit.

You can visit the EICAR website at <http://eicar.com>, read the documentation and download the file from one of the locations on the following web page: http://eicar.com/anti_virus_test_file.htm.

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



Note

The reason we do not include the file in the package is that we want to avoid generating any false alarms for those who use BitDefender or any other virus scanner. You can keep the `EICAR.COM` in a safe place and periodically test the server protection.

5.5. Exclude Folders from Scanning

Depending on the configuration of the system **BitDefender for File Servers** is installed on, some specific files and folders must be excluded from **both on-access and on-demand scanning**. For each software configuration from the following list that applies to your system, check the corresponding section to see what to exclude:

- Computers Running Windows Server 2003, Windows 2000 or Windows XP
- Computers Running Windows Server 2003 and Windows 2000 Domain Controllers
- BitDefender for File Servers and Mail Servers. BitDefender for Mail Servers (WIN SMTP Proxy)
- BitDefender for File Servers and Microsoft Exchange Server
- BitDefender for File Servers and Microsoft ISA Servers
- BitDefender for File Servers and Microsoft SharePoint
- BitDefender for File Servers and BitDefender Enterprise Manager



Computers Running Windows Server 2003, Windows 2000 or Windows XP

The following files and folders must be excluded from both **real-time** and **on-demand** scanning!



Note

`%SystemRoot%`, `%SystemDrive%`, `%ProgramFiles%` are system variables dependent on the operating system and computer configuration. They can be determined using the command SET.

Exclude Microsoft Windows Update or Automatic Update related files:

- The Windows Update or Automatic Update database file:

`%SystemRoot%\SoftwareDistribution\Datastore\Datastore.edb`

- The transaction log files: `Edb*.log` (the wildcard character indicates that there may be several files), `Res1.log`, `Res2.log`, `Edb.chk`, `Tmp.edb`.

These files are located in the following folder:

`%SystemRoot%\SoftwareDistribution\Datastore\Logs\`

Computers Running Windows Server 2003 and Windows 2000 Domain Controllers

The following files and folders must be excluded from both **real-time** and **on-demand** scanning!



Note

`%SystemRoot%`, `%SystemDrive%`, `%ProgramFiles%` are system variables dependent on the operating system and computer configuration. They can be determined using the command SET.



Warning

Serious problems might occur if you modify registry entries incorrectly by using Registry Editor or another method! These problems might require reinstallation of the operating system! Registry keys are given here for the sole purpose of informing you about the location of some files and not to modify them.

- Exclude Active Directory and Active Directory-related files:

1. Main NTDS database files: `Ntds.dit` and `Ntds.pat`.

The location of these files is specified in the following registry key:

`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\DSA Database File`

The default location is:



```
%SystemRoot%\ntds\
```

2. Active Directory transaction log files: Edb*.log (the wildcard character indicates that there may be several files), Res1.log, Res2.log and Ntds.pat (Microsoft Windows Server 2003 no longer uses this last file).

The location of these files is specified in the following registry key:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\Database  
Log Files Path
```

The default location is:

```
%SystemRoot%\ntds\
```

3. The NTDS Working folder: the Temp.edb and Edb.chk files.

The location of these files is specified in the following registry key:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\DSA  
Working Directory
```

- Exclude SYSVOL files:

1. The File Replication Service (FRS) Working folder: FRS Working Dir\jet\sys\edb.chk, FRS Working Dir\jet\ntfrs.jdb and FRS Working Dir\jet\log*.log (the wildcard character indicates that all files having the .log extension will be excluded).

The location of these files is specified in the following registry key:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NtFrs\Parameters\Working  
Directory\
```

2. The FRS Database Log files: *.log (the wildcard character indicates that all files having the .log extension will be excluded).

The location of these files is specified in the following registry key:

```
HKEY_LOCAL_MACHINE\system\currentcontrolset\services\NtFrs\Parameters\DB  
Log File Directory
```

If the registry key is not set, exclude the following files:

```
FRS Working Dir\jet\log\*.log
```

3. The Staging folder

The location of this folder is specified in the following registry key:

```
HKEY_LOCAL_MACHINE\system\currentcontrolset\services\NtFrs\Parameters\Replica  
Sets\GUID\Replica Set Stage
```

The current location of the Staging folder and all of its sub-folders is the file system reparse target of the replica set staging folders. Staging defaults to the following location:



```
%SystemRoot%\sysvol\staging areas\
```

The current location of the SYSVOL\SYSVOL folder and all of its sub-folders is the file system reparse target of the replica set root. The SYSVOL\SYSVOL folder defaults to the following location:

```
%SystemRoot%\sysvol\sysvol\
```

4. The FRS Preinstall folder

The location of this folder is specified in the following registry key:

```
Replica_root\DO_NOT_REMOVE_NtFrs_PreInstall_Directory\
```

The Preinstall folder is always open when FRS is running.

In summary, the targeted and excluded list of folders for a SYSVOL tree that is placed in its default location would look similar to the following:

Folder	Action
%systemroot%\sysvol\	Exclude
%systemroot%\sysvol\domain\	Scan
%systemroot%\sysvol\domain\DO_NOT_REMOVE_NtFrs_PreInstall_Directory\	Exclude
%systemroot%\sysvol\domain\Policies\	Scan
%systemroot%\sysvol\domain\Scripts\	Scan
%systemroot%\sysvol\staging\	Exclude
%systemroot%\sysvol\staging areas\	Exclude
%systemroot%\sysvol\sysvol\	Exclude

If any of these folders or files has been moved or placed in a different location, scan or exclude the equivalent element.

- DFS

The same resources that are excluded for a SYSVOL replica set must also be excluded when FRS is used to replicate shares that are mapped to the DFS root and link targets on Windows 2000 or Windows Server 2003-based member computers or domain controllers.

Note



For more information, see Microsoft KB article: <http://support.microsoft.com/kb/822158/>.



BitDefender for File Servers and Mail Servers. BitDefender for Mail Servers (WIN SMTP Proxy)

The following files and folders must be excluded from both **real-time** and **on-demand** scanning!

Note



`%SystemRoot%`, `%SystemDrive%`, `%ProgramFiles%` are system variables dependent on the operating system and computer configuration. They can be determined using the command SET.

- If **BitDefender for File Servers** is installed on the same machine as the mail server, exclude the following folders:
 1. the folder where the mail server is installed;
 2. the folder where the mailboxes and mail queues are stored.
- If **BitDefender for File Servers** is installed on the same machine as **BitDefender for Mail Servers (WIN SMTP Proxy)**, exclude the folder where BitDefender creates its temporary files:

`%SystemRoot%\Temp\BDNP\`

Note



`%SystemRoot%`, `%SystemDrive%`, `%ProgramFiles%` are system variables dependent on the operating system and computer configuration. They can be determined using the command SET.

BitDefender for File Servers and Microsoft Exchange Server

The following files and folders must be excluded from both **real-time** and **on-demand** scanning!

Note



`%SystemRoot%`, `%SystemDrive%`, `%ProgramFiles%` are system variables dependent on the operating system and computer configuration. They can be determined using the command SET.

- If **BitDefender for File Servers** is installed on the same machine as **BitDefender for MS Exchange**, exclude the folder where BitDefender creates its temporary files:
 - `%ProgramFiles%\Softwin\Temp\`
 - `%SystemRoot%\Temp\BDNP\` (BitDefender for MS Exchange 2003 and 2000 only)
- Exclude Exchange databases and log files across all storage groups. The default location is:

`\Exchsrvr\Mdbdata\`



- Exclude Exchange `.mta` files. The default location is:
`\Exchsrvr\Mtadata\`
- Exclude the additional log files such as
`\Exchsrvr\Server_name.log`
- Exclude virtual server folder. The default location is:
`\Exchsrvr\Mailroot\`
- Exclude the working folder that is used to store streaming `.tmp` files that are used for message conversion. The location is configurable. The default location is:
`\Exchsrvr\Mdbdata\`
- Exclude the **temporary folder** that is used in conjunction with offline maintenance utilities, like **Eseutil.exe**. By default, this folder is the location where the `.exe` file is run from, but you can configure where you run the file when you run the utility.
- Exclude Site Replication Service (SRS) files from the folder:
`\Exchsrvr\Srsdata\`
- Exclude Internet Mail Connector files. The default location is:
`\Exchsrvr\IMCData\`
- Exclude Microsoft Internet Information Service (IIS) system files. The default location is:
`%SystemRoot%\System32\Inetsrv\`
- Exclude the **folder** that contains the `.chk` (Checkpoint) files.

**Note**

Even if you move Exchange databases and log files to new locations and exclude those folders, the `.chk` file may still be scanned.

- **Only for Exchange 5.5!**
Exclude the following file types: `.edb` and `.log`.
- **Only for Exchange 2000!**
 1. Exclude **drive M**.
 2. Exclude the following file types: `.edb`, `.stm` and `.log`.
 3. If you use Microsoft BackOffice POP3 Connector to pull emails from an external POP3 account, exclude the incoming mail folder. The default location is:
`%ProgramFiles%\Microsoft BackOffice\Connectivity\POP3 Connector\Incoming\`
- **Only for Exchange 2003!**



1. If you use Microsoft BackOffice POP3 Connector to pull emails from an external POP3 account, exclude the incoming mail folder. The default location is:

```
%ProgramFiles%\Microsoft Windows Small Business
Server\Networking\POP3\Incoming Mail\
```

2. Exclude the Internet Information Services (IIS) 6.0 compression folder that is used with Outlook Web Access 2003. The default location is:

```
%SystemRoot%\IIS Temporary Compressed Files\
```

3. For clusters, exclude:

```
Quorum disk
%Winnt%\Cluster folder\
\Exchsrvr\Conndata folder\
```

4. If the antivirus supports scanning processes feature, exclude the following processes from scanning: **Cdb.exe**, **Cidaemon.exe**, **Store.exe**, **Emsmta.exe**, **Mad.exe**, **Msearch.exe**, **Inetinfo.exe** and **W3wp.exe**.

You may want to exclude the whole **Exchsrvr** folder from scanning.



Note

Microsoft strongly recommends that you **temporarily disable** file-based scanning software during **operating system and Exchange upgrades**; this includes upgrading to new versions of Exchange and the operating system, and applying any Exchange or operating system fixes or service packs.

For more information see the following Microsoft KB articles:

<http://support.microsoft.com/kb/823166>

<http://support.microsoft.com/kb/328841>

<http://support.microsoft.com/kb/245822/>

BitDefender for File Servers and Microsoft ISA Servers

The following files and folders must be excluded from both **real-time** and **on-demand** scanning!



Note

`%SystemRoot%`, `%SystemDrive%`, `%ProgramFiles%` are system variables dependent on the operating system and computer configuration. They can be determined using the command SET.

If **BitDefender for File Servers** is installed on the same machine as **BitDefender for MS ISA Servers**, exclude the folder where BitDefender creates its temporary files:

```
\%SystemRoot%\Temp\BDNP
```

Where `%SystemRoot%` is:



- \Winnt\ - for Windows 2000;
- \Windows\ - for Windows 2003 and ISA 2000.
- **the Network Service profile**, which is usually located in %SystemDrive%\Documents and Settings\NetworkService\Local Settings\ - for Windows 2003 and ISA 2004, 2006.

BitDefender for File Servers and Microsoft SharePoint

The following files and folders must be excluded from both **real-time** and **on-demand** scanning!



Note

%SystemRoot%, %SystemDrive%, %ProgramFiles% are system variables dependent on the operating system and computer configuration. They can be determined using the command SET.

- If **BitDefender for File Servers** is installed on the same machine as **BitDefender for MS SharePoint**, exclude the folder where BitDefender creates its temporary files:

```
%SystemRoot%\Temp\BDTemp\
```

- To increase server performance, you should exclude the SharePoint databases. To find them, it is usually necessary to follow a path of the following form:

```
%ProgramFiles%\Microsoft SQL Server\
```

BitDefender for File Servers and BitDefender Enterprise Manager

The following files and folders must be excluded from both **real-time** and **on-demand** scanning!



Note

%SystemRoot%, %SystemDrive%, %ProgramFiles% are system variables dependent on the operating system and computer configuration. They can be determined using the command SET.

- To increase server performance, exclude the Enterprise Manager working folder:
%ProgramFiles%\Softwin\BitDefender Enterprise Manager\BitDefender Server\.

5.6. Remove BitDefender for File Servers

Removing, Repairing or Modifying BitDefender

If you want to modify, repair or remove **BitDefender for File Servers**, access the Windows start menu and follow this path: **Start** → **Programs** → **BitDefender for File Servers** → **Modify, Repair or Uninstall**.



You will be requested to confirm your choice by clicking **Next**. A new window will appear where you can select:

- **Modify** - to select new program components to be added or to select currently installed components to be removed;
- **Repair** - to re-install all program components installed during the previous setup;
- **Remove** - to remove all installed components.

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

Uninstalling BitDefender Manually

To manually uninstall **BitDefender for File Servers** you first need to remove some BitDefender components (mainly services). The order is reverse to that of the manual installation:

On-Demand Scan Module

Default path: `\Program Files\Softwin\BitDefender for File Servers\fsdemand.exe`.

Unregister the On-Demand Scan Module using the following command:
fsdemand unregister.

BitDefender Console

Default path: `\Program Files\Common Files\Softwin\Console\bdconsole.dll`.

Unregister the BitDefender Console using the following command: **regsvr32 -u bdconsole.dll**.

BitDefender for File Servers Service

Default path: `\Program Files\Softwin\BitDefender for File Servers\bdfs.exe`.

To remove this service, enter the following commands in the shell:

1. **bdfs /stop** - stop the service.
2. **bdfs /uninstall** - remove the application from the Windows Services.
3. **bdfs /unregister** - remove the service from the BitDefender registry.

BitDefender Live Update Service

Default path: `\Program Files\Common Files\Softwin\bdlived.exe`.

To remove this service, enter the following commands in the shell:

1. **bdlived uninstall** - remove the application from the Windows Services.
2. **bdlived unregister** - remove the service from the BitDefender registry.



BitDefender Statistics Service

Default path: `\Program Files\Common Files\Softwin\Stats\BDStat.exe`.

To stop and remove this service, enter the following commands in the shell:

1. **BDStat /stop** - stop the service.
2. **BDStat /uninstall** - remove the application from the Windows Services.

BitDefender Logging Service

Default path: `\Program Files\Common Files\Softwin\bdlogd.exe`.

The BitDefender Logging Service manages and logs the information sent by agents using four plugins: `filelog.npl`, `mn-smtp.npl`, `winnt.npl` and `rtvr.npl`. These plugins are located by default in: `\Program files\Common Files\Softwin\BDLog`.

To stop and remove this service, enter the following commands in the shell:

1. **bdlogd stop** - stop the service.
2. **bdlogd uninstall** - remove the application from the Windows Services.
3. **bdsetup uninstall "rtvr.npl full path" "rtvr.npl installation path"** - uninstall the plugin. You must specify the path to the file (full or relative) and the full installation path.

Note



Example: **bdsetup uninstall "/BDLog/rtvr.npl" "C:\Program Files\Common Files\Softwin\BDLog"**

4. **bdsetup -u "nn-winnt.npl installation path"** - uninstall the plugin. You must specify the full installation path.

Note



Example: **bdsetup -u "C:\Program Files\Common Files\Softwin\BDLog"**

5. **bdsetup uninstall "mn_smtp.npl full path" "mn_smtp.npl installation path"** - uninstall the plugin. You must specify the path to the file (full or relative) and the full installation path.

Note



Example: **bdsetup uninstall "/BDLog/mn_smtp.npl" "C:\Program Files\Common Files\Softwin\BDLog"**

6. **bdsetup uninstall "filelog.npl full path" "filelog.npl installation path"** - uninstall the plugin. You must specify the path to the file (full or relative) and the full installation path.

**Note**

Example: `bdsetup uninstall "/BDLog/filelog.npl" "C:\Program Files\Common Files\Softwin\BDLog"`

7. **bdlogd unregister** - remove the service from the BitDefender registry.

BitDefender Scanning Service

Default path: `\Program Files\Common Files\Softwin\bdscand.exe`.

To stop and remove this service, enter the following commands in the shell:

1. **bdscand stop** - stop the service.
2. **bdscand uninstall** - remove the application from the Windows Services.
3. **bdscand unregister** - remove the service from the BitDefender registry.

BitDefender Registry Service

Default path: `\Program Files\Common Files\Softwin\BDReg\bdregsvr2.exe`.

Currently, there is no command to remove this service due to a bug in the product. Find an appropriate tool to remove it.

Finally, after you have removed these BitDefender components, you must also remove:

- the `xreglib.dll` file from `\system32`;
- the `\Program Files\Softwin\BitDefender for File Servers` folder, which contains the BitDefender for File Servers specific files;
- if you do not have other BitDefender products for Windows servers installed, the `\Program Files\Common Files\Softwin\` folder, which contains files common to all BitDefender products for Windows servers.



6. License Key System

A license key allows one user to use **BitDefender for File Servers** during a certain period of time.

6.1. Key Types

There are four types of keys:

- **Trial**
- **End User**
- **OEM**
- **NFS (not for sale)**

The keys can expire:

- On a fixed date – date keys
- After a specific interval starting from the date the product was registered – interval keys.

By default, the installation kit is preregistered with a 30 days trial key. During this period the product can be registered with an End User, OEM or NFS key.



Important

Do not use Trial keys for promotion or events! Use instead End User keys that expire at a specific date.



Note

Keys from File Server version 1.9 of are accepted, but it is strongly advised to use a 2.0 key, because older keys might not be supported in the future.

6.2. Registration Rules

When registering a product, the following rules must be observed:

- If the product is registered with a Trial key, the user can only enter an End User, OEM or NFS key.
- If the product is registered with an End User key, the user can only enter another End User key or an NFS key.
- If the product is registered with an OEM key, the user can only enter an End User key or an NFS key.
- If the product is registered with an NFS key, the user can only enter an End User key.



6.3. Key Authentication

Keys are authenticated by the BitDefender Keys Server. Authentication means checking whether keys are valid or not:

- For interval keys, the license period is counted from the first authentication event (usually when the product is first registered). If another client uses the same key, the same expire dates are applied.
- For date keys, the license period lasts until the predefined date.

How authentication works

BitDefender for File Servers Service sends the key to the BitDefender Keys Server to be authenticated. Based on the server response, the product will be registered, continue to be registered, expire or be invalidated.

Authentication is performed:

- When BitDefender for File Servers Service is (re)started
- When key settings are changed in the product console
- Once a day, when BitDefender for File Servers Service runs continuously.

Note



Only End User and NFS keys can be authenticated.

If an error appears in the authentication process (connection fails or errors in sending the key and receiving the answer), the validity of the key is locally computed. This means that the original license period/date of the key is used.

Extending the license period

BitDefender for File Servers supports license period extension through authentication. This means that the license period of a product can be extended by extending the validity of the key from BitDefender Key Server. When the product is authenticated, the new expiration time will be sent.

Note



In case of an authentication error, the extended key will not work until the next successful authentication.

Note



BitDefender for File Servers does not support license period extension by introducing a new key. This means that if the product is registered with a new key before the old key expires, the license period will be the one of the new key. Example: Let's assume that Key 1 expires in 3 months and the product is registered with a new key which expires in 12 months. As a result the product will expire in 12 months.



7. Enterprise Integration

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

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

7.1. BitDefender Enterprise Manager Integration Advantages

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



Important

In order to use additional BitDefender for File Servers task templates, you must import them from a BitDefender Enterprise Manager client that has BitDefender for File Servers installed.

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

Configure BitDefender for File Servers.

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

Get BitDefender Client Status (servers).

- Offers a list of the entire configuration of the BitDefender for File Servers client, which is to be found in the **Active Tasks** section. By running the task one-time only, it is possible to acquire information about one or more clients.
- Offers centralized information on all BitDefender for File Servers clients by generating reports based on the results of this task. The report can be generated periodically, printed or exported in HTML format for further information processing.



Get BitDefender for File Servers Statistics.

- Offers general or specific information about the activity of the BitDefender for File Servers client, in a selected time interval. By running the task one time only, it is possible to acquire information about one or more clients.
- Monitors the activity of a single client or of all the BitDefender for File Servers clients, by generating reports based on the results of this task. The report can be generated periodically, printed or exported in HTML format for further information processing.
- Provides an overview of the global protection of all file servers in the organization.
- Offers the possibility of passing the product activity monitoring task from the local admin of the file server on to the admin of BitDefender for File Servers.

Scan Computer (FileServer).

- Initiates on-demand scanning processes on one or all BitDefender for File Servers clients.
- Provides centralized scheduling capabilities for all BitDefender for File Servers clients. The scan process can be performed on a regular basis on all clients when the machines are in the idle mode.

Update BitDefender.

- Initiates update processes on one or all BitDefender for File Servers clients.
- Provides centralized scheduling capabilities for all BitDefender for File Servers clients. The update process can be performed on a regular basis on all clients, taking into consideration the work schedule and the internal policy.

7.2. BitDefender for File Servers Server Add-on

BitDefender Enterprise Manager comes with a **BitDefender for File Servers Server Add-on**, which contains increased management capabilities for **BitDefender for File Servers**.



Important

If you choose to install the **BitDefender for File Servers Server Add-on**, you will not have to import the BitDefender for File Servers tasks. These tasks, along with other additional tasks that come with the Add-on, will appear by default in the **Task Templates** section.

Besides the tasks previously described, the BitDefender for File Servers Server Add-on contains several other additional tasks:

Apply BitDefender for File Servers Patch.

- Provides centralized management of the product updates.



- Ensures that all BitDefender for File Servers products are up to date, without interfering with the servers activity. The patches can be applied when the machines are in the idle mode.
- Offers the possibility of passing the product update task from the local admin of the file server on to the admin of BitDefender for File Servers.

Install BitDefender for File Servers.

- Allows installing BitDefender for File Servers on one ore more BitDefender Enterprise Manager clients. This can be made by running this single task one-time only.
- Offers the possibility of scheduling the installation at a time when the machines are in the idle mode so as not to interfere with the server activity.
- Offers the possibility to deploy BitDefender for File Servers and BitDefender Local Manager at the same time.

Install BitDefender for File Servers (automatically restart target machines if needed).

- Beside the advantages offered by the previous task, it allows the complete installation of BitDefender for File Servers by automatically restarting the target machines, if necessary.

Uninstall BitDefender for File Servers.

- Allows uninstalling BitDefender for File Servers from the selected clients. This can be done by running this single task one-time only.
- Offers the possibility to schedule the removal process at a time when the machines are in the idl mode so as not to interfere with the server activity.

Uninstall BitDefender for File Servers (automatically restart target machines if needed).

- Beside the advantages offered by the previous task, it allows the complete removal of BitDefender for File Servers by automatically restarting the target machines, if necessary.



8. BitDefender Windows Servers Registry Keys

The BitDefender Registry is a vital component of **all BitDefender products for Windows servers**. Its role is to store and manage the product settings, ensuring the functionality of the product.

Two important components define the BitDefender Registry:

- the **BitDefender Registry Service**;
- the **settings file** (`xdb.xml`).

The **BitDefender Registry Service** manages the BitDefender settings. It receives requests from BitDefender components to read data from the **settings file** or to write data in this file. For example, when a component is registered, it sends its default settings to the BitDefender Registry Service, which writes them in the `xdb.xml` file. Therefore, all BitDefender components depend on this service.

The **settings file** (`xdb.xml`) is a database which stores the product settings. The keys contain settings that are grouped into two categories:

- common settings, used by all BitDefender products for Windows servers.
- specific settings, used solely by a certain BitDefender product for Windows servers: in our case, this is **BitDefender for File Servers**.

During the registration of the BitDefender components, the **BitDefender Registry Service** writes the default product settings in this file. Then, the file is automatically modified by the **BitDefender Registry Service** whenever the latter receives a request to write data from the BitDefender components.

The registry keys from `xdb.xml` can also be modified manually. This is necessary when the product does not work properly and needs debugging.

To edit the database manually, please follow the next steps:

1. End the **BitDefender Registry Service** (use the **Windows Task Manager** or other means).



Note

Currently, there is no command to end this service from a shell due to a bug in the product.

2. Open `xdb.xml`, make the necessary changes and save the file.
3. Start the **BitDefender Registry Service**.

**Important**

The database cannot be modified while the service is running!

8.1. Important Registry Keys

Each change in the **settings file** is reflected in the way the product works. As a consequence, an incorrect key value may cause a fault in the product. That is why knowing some of the important registry keys can help debug the product.

**Note**

To see the complete list of BitDefender registry keys along with a short description, please check the "[Appendix A - Registry Keys](#)" (p. 52) section.

Further on, the main registry keys will be presented. These keys concern:

Product versions. There are two main keys that offer information about the version of a product or product component:

- `NetProtect/Versions/` - contains subkeys that provide information about the version of the product, the agent and the BitDefender Statistics service.

The name and version of BitDefender for File Servers is stored in the following key:

```
NetProtect/Versions/FileServer/
```

- `BDUX/Versions/` - contains subkeys that provide information about the version of the Scanning, Live Update and Logging services.

BitDefender agents. Agents are the main modules of a product. They coordinate the work specific to the product: catch files / mails and send them to core to be scanned, provide information for logs and statistics, etc. Each product has one agent: in our case, this is **BitDefender for File Servers**.

The BitDefender for File Servers agent settings are stored in several keys located in the `NetProtect/Agents/FileServer/` main key. Here are some of the most important keys:

- `NetProtect/Agents/FileServer/Key/` - stores information about the license key.
- `NetProtect/Agents/FileServer/RTP/` - stores the settings for the real-time protection module.

The `NetProtect/Agents/FileServer/RTP/Enabled/` key sets the status of the real-time protection: enabled if its value is `Y` or disabled if it is `N`.

- `NetProtect/Agents/FileServer/ODS/` - stores the settings for the on-demand scan module.



The `Y` value of the `NetProtect/Agents/FileServer/ODS/Busy/` key indicates that an on-demand scan is running. Only one instance of the on-demand scanner is permitted.

The `NetProtect/Agents/FileServer/ODS/Cancel/` key is used to cancel a scan process. The `Y` value of this key stops the current on-demand scan.

Logger plugins. The BitDefender Logging service uses four plugins to manage the information sent by agents. Its settings are stored in the `BDUX/LoggerDaemon/`, while the plugin settings can be found in the subkeys of `BDUX/LoggerDaemon/Plugins/`:

- `BDUX/LoggerDaemon/Plugins/RTVR/` - stores the settings for the real-time virus report (RTVR) module. Two keys require your attention:

- `BDUX/LoggerDaemon/Plugins/RTVR/Active/`

Depending on the value of this key, the plugin is loaded (`Y`) or not (`N`) by the logger service. By default, its value is `Y`.



Note

This key **cannot** be modified through the management console. However, it can be manually modified in `xdb.xml` when needed; e.g.: to see if a problem is generated by the plugin, set its value to `N` in order not to load the plugin.

- `BDUX/LoggerDaemon/Plugins/RTVR/Enable/`

Stores the status of the plugin: `Y` for enabled or `N` for disabled. It shows whether the plugin is being used or not by the logger. Regardless of its value, the plugin is always loaded if the value of the `Active` key is `Y`.



Note

This key is usually modified through the management console when the user enables / disables the interface option corresponding to the plugin.

- `BDUX/LoggerDaemon/Plugins/Filelog/` - stores the settings for the file log plugin. This logger plugin creates the log file on the disk. Two keys require your attention:

- `BDUX/LoggerDaemon/Plugins/Filelog/Active/`

Depending on the value of this key, the plugin is loaded (`Y`) or not (`N`) by the logger service. By default, its value is `Y`.



Note

This key **cannot** be modified through the management console. However, it can be manually modified in `xdb.xml` when needed; e.g.: to see if a problem is generated by the plugin, set its value to `N` in order not to load the plugin.

- `BDUX/LoggerDaemon/Plugins/Filelog/Enable/`



Stores the status of the plugin: **Y** for enabled or **N** for disabled. It shows whether the plugin is being used or not by the logger. Regardless of its value, the plugin is always loaded if the value of the `Active` key is **Y**.

Note

This key is usually modified through the management console when the user enables / disables the interface option corresponding to the plugin.

- `BDUX/LoggerDaemon/Plugins/MNsmtp/` - stores the settings for the mail alert plugin. Two keys require your attention:
 - `BDUX/LoggerDaemon/Plugins/MNsmtp/Active/`

Depending on the value of this key, the plugin is loaded (**Y**) or not (**N**) by the logger service. By default, its value is **Y**.

Note

This key **cannot** be modified through the management console. However, it can be manually modified in `xdb.xml` when needed; e.g.: to see if a problem is generated by the plugin, set its value to **N** in order not to load the plugin.

- `BDUX/LoggerDaemon/Plugins/MNsmtp/Enable/`

Stores the status of the plugin: **Y** for enabled or **N** for disabled. It shows whether the plugin is being used or not by the logger. Regardless of its value, the plugin is always loaded if the value of the `Active` key is **Y**.

Note

This key is usually modified through the management console when the user enables / disables the interface option corresponding to the plugin.

- `BDUX/LoggerDaemon/Plugins/Winnt/` - stores the settings for the net send alert plugin. Two keys require your attention:
 - `BDUX/LoggerDaemon/Plugins/Winnt/Active/`

Depending on the value of this key, the plugin is loaded (**Y**) or not (**N**) by the logger service. By default, its value is **Y**.

Note

This key **cannot** be modified through the management console. However, it can be manually modified in `xdb.xml` when needed; e.g.: to see if a problem is generated by the plugin, set its value to **N** in order not to load the plugin.

- `BDUX/LoggerDaemon/Plugins/Winnt/Enable/`



Stores the status of the plugin: `Y` for enabled or `N` for disabled. It shows whether the plugin is being used or not by the logger. Regardless of its value, the plugin is always loaded if the value of the `Active` key is `Y`.

**Note**

This key is usually modified through the management console when the user enables / disables the interface option corresponding to the plugin.

Live update. The settings for the BitDefender Live Update service can be found in the `BDUX/LiveDaemon/` key. The following subkeys require your attention:

- `BDUX/LiveDaemon/ProxyOn/`
Indicates if a proxy is used to connect to the update server (`Y` value) or not (`N` value). The proxy settings are stored in the `BDUX/LiveDaemon/ProxySettings/` key.
- `BDUX/LiveDaemon/CheckSecs/`
Sets the time interval to check for updates.
- `BDUX/LiveDaemon/MainLocation/`
Specifies the location from where to download the updates.
- `BDUX/LiveDaemon/LastCheck/`
Stores the time when the last check for updates was performed.
- `BDUX/LiveDaemon/LastUpdate/`
Stores the time when the last update was performed.

BitDefender Scanning service. The settings for this service are contained in `BDUX/ScanDaemon/`. The number of virus signatures currently installed is stored in the `BDUX/ScanDaemon/Signatures/` subkey.



9. File List

The product files can be found in four main folders:

- \Program Files\Softwin\BitDefender for File Servers
- \Program files\Common Files\Softwin
- \System32
- \Program Files\Softwin\BitDefender Enterprise Manager\BitDefender Update Server

9.1. \Program Files\Softwin\BitDefender for File Servers

This folder contains the files that are specific for **BitDefender for File Servers**. It includes the following BitDefender components:

On-Access Scan Module

File list: \Program Files\Softwin\BitDefender for File Servers\bdfs.exe.

This file represents the BitDefender for File Servers service. It ensures that all accessed files are scanned.

On-Demand Scan Module

File list: \Program Files\Softwin\BitDefender for File Servers\fsdemand.exe.

This file is the .exe used for the on-demand scan. It sends the BitDefender Scanning Service the files the user marked for scanning on the interface.

BitDefender Error Report Wizard

File list: \Program Files\Softwin\BitDefender for File Servers - bdch.dll, bdch.ini, bdsbmit.dll, bdsbmit.exe, bdsbmit.ini.

bdsbmit.* are the files of the application that sends the report to the BitDefender Lab: the .exe is the application.

bdch.* are the files that compose the Crash Handler, the wizard which identifies the problem.

BitDefender for File Server Driver

File list: \Program Files\Softwin\BitDefender for File Servers - filespy.sys, filespy9x.dll, fsmon.dll.

These files intercept any event on the local machine (write, read, rename, delete, open) and send the accessed files to the BitDefender for File Servers service.

Product Documentation



The product documentation consists of a single file, `npfs.chm`, which contains explanations on how to use the product and other helpful information.

9.2. \Program files\Common Files\Softwin

This folder contains the files common to **all BitDefender products for Windows servers**. It includes the following BitDefender components:

BitDefender Registry

File list: \Program files\Common Files\Softwin\BDReg - bdregsrv2.exe, xdb.xml, bdregsrv2.pem.

`bdregsrv2.exe` is the communication application which reads, writes or deletes keys from the `xdb.xml` file at the request of other components (console, services).

`xdb.xml` is the database that stores the product settings.

Note



This component also includes the `xreglib.dll` file, a BitDefender Registry dll library, located in the `\System32` folder.

BitDefender Logging Service

File list:

- \Program files\Common Files\Softwin\bdlogd.exe
- \Program files\Common Files\Softwin\BDLog - filelog.npl, mn-smtp.npl, rtvr.npl, winnt.npl, bd.log
- \Program files\Common Files\Softwin\BDLog\Templates*.ptt
- \Program files\Common Files\Softwin\BDLog\Nettemplates*.ptt

`bdlogd.exe` is the application that loads the logger plugins (`filelog.npl`, `mn-smtp.npl`, `rtvr.npl`, `winnt.npl`) in order to manage the information sent by the agent components (the On-access and On-demand scan modules).

The `*.ptt` files from the **Templates** and **Nettemplates** subfolders are the templates used for the mail and net send alerts.

BitDefender Statistics Service

File list: \Program files\Common Files\Softwin\Stats - BDStat.exe, *.ini.

`BDStat.exe` is the application that manages statistics, while the `*.ini` files the respective statistics.

This folder also contains the customized reports created by BitDefender based on the user's preferences (in the **ConsoleReports** subfolder).

The **Lang** subfolder contains `BDStatLang.dll`, which includes most of the user interface texts related to statistics.



BitDefender Scanning Service

File list: \Program files\Common Files\Softwin\bdscand.exe.

It scans files using the BitDefender antivirus engines and plugins.

BitDefender Scheduler Service

File list: \Program files\Common Files\Softwin\BDScheduler.exe.

It schedules scan and update tasks and it indicates to the corresponding services when to perform the respective task.

BitDefender Local Manager

File list: \Program files\Common Files\Softwin\npemclient.exe

This file ensures the integration of BitDefender for File Servers with BitDefender Enterprise Manager. It is not installed by default.

Note



To integrate BitDefender for File Servers with BitDefender Enterprise Manager, the BitDefender Local Manager must be deployed on the local machine.

BitDefender Setup

File list: \Program files\Common Files\Softwin\bdsetup.exe

The application registers and unregisters the BitDefender components in and from the BitDefender Registry.

Content Filter

File list: \Program files\Common Files\Softwin\CFilter - iconv.dll, NPFfilter.dll

iconv.dll is the general library of the content filter. NPFfilter.dll is the wrapper, an interface between the filter and the product containing specific functions for BitDefender for File Servers.

BitDefender GUI

File list:

- \Program files\Common Files\Softwin\Console: bdconsole.dll, bdconsole.exe, bitdefender.msc.
- \Program files\Common Files\Softwin\Console\Lang: BDConsoleLang.dll.
- \Program files\Common Files\Softwin\Console\HTMLS-antivirusstatus.png, bar.png, bar_left.png, bar_right.png, bd_left.bmp, bd_middle.bmp, bd_right.bmp, button1.bmp, button2.bmp, dot.png, down.gif, down.png, down_left.png, down_right.png, index.html, product update.html, serverstatus.png, status.html, top.gif, top.png, up.png, up_left.png, up_right.png, updatestatus.png.



`bitdefender.msc` represents the MMC interface, `bdconsole.dll` is the dll library and `bdconsole.exe` is the application that starts the console.

The **Lang** subfolder contains the dll which includes most of the user interface texts.

The **HTMLS** subfolder contains the images and the HTML files of the user interface.

BitDefender HTTP Server

File list: `\Program files\Common Files\Softwin\BitDefender HTTP Server - http.exe, httpconfig.xml`.



Note

The folder is created only if the BitDefender Update Server is installed.

`http.exe` publishes the updates locally.

`httpconfig.xml` contains the Update Server settings.

BitDefender Communicator

File list: `\Program files\Common Files\Softwin\BitDefender Communicator - xcommsvr.exe, xgate.dll`.



Note

The folder is created only if the BitDefender Update Server is installed.

These files ensure the communication between BitDefender for File Servers and BitDefender Enterprise Manager.

Antivirus Engine

File list:

- `\Program files\Common Files\Softwin\AV - avxdisk.dll, avxs.dll, avxt.dll, bdc.exe, bdc.ini, bdcore.dll, bdupd.dll, label.dat, libfn.dll, plugins.htm, version.dat`.
- `\Program files\Common Files\Softwin\AV\Plugins - *.cvd, *.ivd, *.rvd, *.xmd`

`bdcore.dll` is the core library, `bdc.ini` is the configuration file of the core and `bdc.exe` is the core.

The **Plugins** subfolder contains the antivirus plugins.

GUI texts

The texts from the GUI for the most of the BitDefender components are contained in the files from: `\Program files\Common Files\Softwin\Lang`.



9.3. \System32

This folder contains some auxiliary files (system files) used by BitDefender, namely: `mfc71.dll`, `mfc71u.dll`, `msvcp70.dll`, `msvcp71.dll`, `msvcr71.dll`, `mfc70.dll` and `msvcr70.dll`.

`xreglib.dll`, a BitDefender Registry dll library, and `xcomm.dll`, the BitDefender Local Manger dll library, are also located here.

9.4. \Program Files\Softwin\BitDefender Enterprise Manager\BitDefender Update Server

This folder contains some of the files used by BitDefender Update Server, namely: `bdupdconfig.exe`, `bdupdsvr.exe`, `BDUPDSVR.ini`, `httpgetfile.dll`, `updprod.ini`.

`bdupdconfig.exe` is the wizard that assists the user in configuring the settings for the Update Server.

`bdupdsvr.exe` is the application that searches for updates.



Note

This folder is only created if the BitDefender Update Server component is installed.



10. Troubleshooting

10.1. Changing the Configuration

- In the default configuration, certain versions of BitDefender for File Servers scan all files on-access, regardless of their size. To check this setting, open the console, click **Antivirus**, then **On-access Scanner**, and, finally, **Configure BitDefender On-Access Scanner**. If the maximum file size is set to 0, click the **Change** button to specify a convenient size.
- In the default configuration, BitDefender for File Servers moves to quarantine any infected file discovered. It is not recommended to use the **Delete** or the **Ignore** actions in the on-access protection.
- In the default configuration, BitDefender for File Servers deletes any infected file discovered during an on-demand scan. When configuring the on-demand scan, it is recommended to set the actions to **Disinfect** and **Move to quarantine**.
- When installing BitDefender for File Servers, it is recommended to exclude mail storages and databases from the on-access scanning process. Open the console, click **Antivirus**, then **On-access Scanner**, next **Configure BitDefender On-Access Scanner**. In **Scan all files or folders** click **Change...**, and select **Custom Scan**. Select all the folders you want to exclude from the on-access scanning. For specific configurations, refer to the appropriate articles at: <http://kb.bitdefender.com/P33-0-en--Browse-by-BitDefender-for-FileServer.html>.

10.2. Changing the Number of Scanning Threads

Increasing or reducing the number of scanning threads can improve the performance of your file server. The default value is 4.

To increase the number of scanning threads:

1. Open a **Command Prompt** window and change the current working directory to folder `%CommonProgramFiles%\Softwin\`.
2. Type the command:

```
bdsetup.exe setkey "/BDUX/ScanDaemon/Variator/Min" "<Threads>"
```

where `<Threads>` represents the number of desired threads.



10.3. Stopping the Continuous On-Demand Scan of an Inexistent File

The situation is due to the `<Busy value="Y" />` value in `xdb.xml`. Due to an improperly ended scan, this value remains set on "Y" instead of "N". Follow these steps to correct this situation:

1. Stop the **BitDefender for File Servers** and **BitDefender Scanning Service** services.
2. Open `xdb.xml`, replace the existing Busy and Cancel values as follows:
`<Busy value="N" />`
`<Cancel value="Y" />`
Save the file.
3. Restart the two services.

10.4. Asking for Assistance

In order to better understand the situation you are dealing with please send us the following information:

1. Open **Control Panel**, double-click **Add or Remove Programs**, identify the product, click the link **Click here for support information**, and write down the build number. Repeat this step for each BitDefender product installed on the server.
2. The following files:
`%CommonProgramFiles%\Softwin\xdb.xml`
`%CommonProgramFiles%\Softwin\XLOG\np.log`
If 2.0 generation products are installed, also attach the following files:
`%CommonProgramFiles%\Softwin\BDReg\xdb.xml`
`%CommonProgramFiles%\Softwin\BDLog\bd.log`
3. The **Application** and **System** logs from **Windows Event Viewer** saved in `.evt` format. To access these logs, open **Control Panel**, then **Administrative Tools**, and click **Event Viewer**.
4. The hardware and software configuration of the server. Include reports `sysdump.tar` and `BDFFileInfo.log`.
5. The screenshot of the **Services** window where the BitDefender services names, status, and start-up type are clearly visible.



Note

You can find solutions to many common issues by searching the [BitDefender Knowledge Base](#).



A. Appendix A - Registry Keys

In this appendix you can find all BitDefender registry keys and their description. The keys are sorted alphabetically so as to easily find a specific key.



Note

To find more information about the BitDefender Registry and some of the most important keys, please check the *“BitDefender Windows Servers Registry Keys”* (p. 39) section.

`BDUX/LiveDaemon/`

Contains the settings for the live update service.

`BDUX/LiveDaemon/CheckSecs/`

Stores the time interval to check for updates.

`BDUX/LiveDaemon/LastCheck/`

Stores the time when the last check for updates was performed.

`BDUX/LiveDaemon/LastUpdate/`

Stores the time when the last update was performed.

`BDUX/LiveDaemon/MainLocation/`

Stores the location from where to download the updates.

`BDUX/LiveDaemon/ProxyOn/`

Its value is `y` if a proxy is used to connect to the update server.

`BDUX/LiveDaemon/ProxySettings/`

Stores the proxy settings.

`BDUX/LiveDaemon/UpLocs/en_fs_20/`

Stores the location on the disk where BitDefender for File Servers is updated.

`BDUX/LiveDaemon/UpLocs/update71/`

Stores the location on the disk where the antivirus signatures and engines are updated.

`BDUX/LiveDaemon/Verbose/`

If its value is `y` the verbose (detailed) logs are logged.

`BDUX/LoggerDaemon/`

Contains the settings for the BitDefender Logger.

`BDUX/LoggerDaemon/Plugins/`

Contains the settings for the logger plugins.

`BDUX/LoggerDaemon/Plugins/Filelog/`

Contains the settings for the file log plugin. This logger plugin creates the log file on the disk.



BDUX/LoggerDaemon/Plugins/Filelog/Active/

Depending on the value of this key, the plugin is loaded (Y) or not (N) by the logger service. By default, its value is Y.

Note



This key **cannot** be modified through the management console. However, it can be manually modified in `xdb.xml` when needed; e.g.: to see if a problem is generated by the plugin, set its value to N in order not to load the plugin.

BDUX/LoggerDaemon/Plugins/Filelog/DefaultLogFile/

Stores the default log filename and its default location.

BDUX/LoggerDaemon/Plugins/Filelog/Enable/

Stores the status of the plugin: Y for enabled or N for disabled. It shows whether the plugin is being used or not by the logger. Regardless of its value, the plugin is always loaded if the value of the `Active` key is Y.

Note



This key is usually modified through the management console when the user enables / disables the interface option corresponding to the plugin.

BDUX/LoggerDaemon/Plugins/Filelog/Location/

Stores the location of the log file.

BDUX/LoggerDaemon/Plugins/Filelog/MaxSize/

Stores the maximum size of the log file. If this size is exceeded, the file is overwritten.

BDUX/LoggerDaemon/Plugins/Filelog/Path/

Stores the installation path of the file log plugin.

BDUX/LoggerDaemon/Plugins/MNsmtp/

Contains the settings for the mail alert logger plugin.

BDUX/LoggerDaemon/Plugins/MNsmtp/Active/

Depending on the value of this key, the plugin is loaded (Y) or not (N) by the logger service. By default, its value is Y.

Note



This key **cannot** be modified through the management console. However, it can be manually modified in `xdb.xml` when needed; e.g.: to see if a problem is generated by the plugin, set its value to N in order not to load the plugin.

BDUX/LoggerDaemon/Plugins/MNsmtp/AlertReceivers/

If its value is Y the specified receivers of the mail will be alerted.

BDUX/LoggerDaemon/Plugins/MNsmtp/AlertSender/

If its value is Y the sender of the mail will be alerted.



`BDUX/LoggerDaemon/Plugins/MNsmtp/Enable/`

Stores the status of the plugin: `Y` for enabled or `N` for disabled. It shows whether the plugin is being used or not by the logger. Regardless of its value, the plugin is always loaded if the value of the `Active` key is `Y`.



Note

This key is usually modified through the management console when the user enables / disables the interface option corresponding to the plugin.

`BDUX/LoggerDaemon/Plugins/MNsmtp/Ev<no>/`

Stores the receivers of the mail alerts.

`BDUX/LoggerDaemon/Plugins/MNsmtp/From/`

Stores the address of the user that sends the alerts.

`BDUX/LoggerDaemon/Plugins/MNsmtp/Path/`

Stores the path to the mail alert logger plugin.

`BDUX/LoggerDaemon/Plugins/MNsmtp/SMTPServer/`

Stores the IP of the SMTP server used to send mails (the mails are sent through the SMTP protocol).

`BDUX/LoggerDaemon/Plugins/MNsmtp/Templates/`

Stores the path to the mail templates used for configuring mail alert texts.

`BDUX/LoggerDaemon/Plugins/MNsmtp/Templates/ErrorAlert/`

Stores the path to the error mail alert template.

`BDUX/LoggerDaemon/Plugins/MNsmtp/Templates/FileServerAlert/`

Stores the path to the virus mail alert template.

`BDUX/LoggerDaemon/Plugins/MNsmtp/Templates/InfoAlert/`

Stores the path to the info mail alert template.

`BDUX/LoggerDaemon/Plugins/MNsmtp/Templates/KeyHasExpiredAlert/`

Stores the path to the "key has expired" mail alert template.

`BDUX/LoggerDaemon/Plugins/MNsmtp/Templates/KeyWillExpireAlert/`

Stores the path to the "key will expire" mail alert template.

`BDUX/LoggerDaemon/Plugins/MNsmtp/Templates/OnDemandAlert/`

Stores the path to the on-demand scan mail alert template.

`BDUX/LoggerDaemon/Plugins/MNsmtp/Templates/WarningAlert/`

Stores the path to the warning mail alert template.

`BDUX/LoggerDaemon/Plugins/RTVR/`

Contains the settings for the real-time virus report (RTVR) module.

`BDUX/LoggerDaemon/Plugins/RTVR/Active/`

Depending on the value of this key, the plugin is loaded (`Y`) or not (`N`) by the logger service. By default, its value is `Y`.

**Note**

This key **cannot** be modified through the management console. However, it can be manually modified in `xdb.xml` when needed; e.g.: to see if a problem is generated by the plugin, set its value to `N` in order not to load the plugin.

`BDUX/LoggerDaemon/Plugins/RTVR/Country/`
Stores the country where the reports are sent from.

`BDUX/LoggerDaemon/Plugins/RTVR/Enable/`
Stores the status of the plugin: `Y` for enabled or `N` for disabled. It shows whether the plugin is being used or not by the logger. Regardless of its value, the plugin is always loaded if the value of the `Active` key is `Y`.

**Note**

This key is usually modified through the management console when the user enables / disables the interface option corresponding to the plugin.

`BDUX/LoggerDaemon/Plugins/RTVR/EnableRTSR/`
The `Y` value enables the real-time spam report.

`BDUX/LoggerDaemon/Plugins/RTVR/Hours/`
Stores the frequency (number of hours) of reports.

`BDUX/LoggerDaemon/Plugins/RTVR/Path/`
Stores the installation path of the RTVR plugin.

`BDUX/LoggerDaemon/Plugins/RTVR/Timeout/`
Stores the timeout interval for report sending.

`BDUX/LoggerDaemon/Plugins/RTVR/UID/`
Stores the unique identifier of the machine (UID).

`BDUX/LoggerDaemon/Plugins/RTVR/Viruses/`
Stores the number of viruses found and sent in the report.

`BDUX/LoggerDaemon/Plugins/Winnt/`
Contains the settings for the net send alert logger plugin.

`BDUX/LoggerDaemon/Plugins/Winnt/Active/`
Depending on the value of this key, the plugin is loaded (`Y`) or not (`N`) by the logger service. By default, its value is `Y`.

**Note**

This key **cannot** be modified through the management console. However, it can be manually modified in `xdb.xml` when needed; e.g.: to see if a problem is generated by the plugin, set its value to `N` in order not to load the plugin.

`BDUX/LoggerDaemon/Plugins/Winnt/Enable/`
Stores the status of the plugin: `Y` for enabled or `N` for disabled. It shows whether the plugin is being used or not by the logger. Regardless of its value, the plugin is always loaded if the value of the `Active` key is `Y`.

**Note**

This key is usually modified through the management console when the user enables / disables the interface option corresponding to the plugin.

`BDUX/LoggerDaemon/Plugins/Winnt/Path/`

Stores the path to the net send alert plugin.

`BDUX/LoggerDaemon/Plugins/Winnt/ServerName/`

Stores the name of the server used to send the net send alerts.

`BDUX/LoggerDaemon/Plugins/Winnt/Templates/`

Stores the path to the net send alert templates used to configure net send alert texts.

`BDUX/LoggerDaemon/Plugins/Winnt/Templates/ErrorAlert/`

Stores the path to the error net send alert template.

`BDUX/LoggerDaemon/Plugins/Winnt/Templates/FileServerAlert/`

Stores the path to the virus net send alert template.

`BDUX/LoggerDaemon/Plugins/Winnt/Templates/InfoAlert/`

Stores the path to the info net send alert template.

`BDUX/LoggerDaemon/Plugins/Winnt/Templates/KeyHasExpiredAlert/`

Stores the path to the "key has expired" net send alert template.

`BDUX/LoggerDaemon/Plugins/Winnt/Templates/KeyWillExpireAlert/`

Stores the path to the "key will expire" net send alert template.

`BDUX/LoggerDaemon/Plugins/Winnt/Templates/OnDemandAlert/`

Stores the path to the on-demand scan net send alert template.

`BDUX/LoggerDaemon/Plugins/Winnt/Templates/WarningAlert/`

Stores the path to the warning net send alert template.

`BDUX/NPCFFilter/`

Contains the settings of the content filter.

`BDUX/NPCFFilter/Path/`

Stores the filename, along with the full path of the content filter module.

`BDUX/ScanDaemon/`

Contains the settings for the BitDefender Scanning service.

`BDUX/ScanDaemon/Core/`

Stores the path to the core files of the engines.

`BDUX/ScanDaemon/Plugins/`

Stores the path where the antivirus plugins are located.

`BDUX/ScanDaemon/Quarantine/`

Stores the path to the quarantine folder.



BDUX/ScanDaemon/Signatures/

Stores the number of virus signatures currently installed.

BDUX/ScanDaemon/Variator/

BDUX/ScanDaemon/Variator/Max/

BDUX/ScanDaemon/Variator/MaxThreshold/

BDUX/ScanDaemon/Variator/Min/

BDUX/ScanDaemon/Variator/MinThreshold/

BDUX/ScanDaemon/Variator/Sleep/

BDUX/ScanDaemon/Variator/Steps/

BDUX/Synchronization/

Stores the synchronization keys, which prevent simultaneous reading and writing of the same registry key. Do not change these settings.

BDUX/Versions/

Contains information about the versions of important modules. This information can be seen in the **About** section from the management console.

BDUX/Versions/LiveDaemon/

Contains information about the BitDefender Live Update service version.

BDUX/Versions/LiveDaemon/Name/

Stores the service name. This information can be seen in the **About** section from the management console.

BDUX/Versions/LiveDaemon/Version/

Stores the service version. This information can be seen in the **About** section from the management console.

BDUX/Versions/LoggerDaemon/

Contains information about the BitDefender Logging service version.

BDUX/Versions/LoggerDaemon/Name/

Stores the service name. This information can be seen in the **About** section from the management console.

BDUX/Versions/LoggerDaemon/Version/

Stores the service version. This information can be seen in the **About** section from the management console.

BDUX/Versions/ScanDaemon/

Contains information about the BitDefender Scanning service version.

BDUX/Versions/ScanDaemon/Name/

Stores the service name. This information can be seen in the **About** section from the management console.



`BDUX/Versions/ScanDaemon/Version/`

Stores the service version. This information can be seen in the **About** section from the management console.

`NetProtect/Agents/`

Contains the settings for agents.

Agents are the main modules of a product. They coordinate the work specific to the product: catch files / mails and send them to core to be scanned, provide information for logs and statistics, etc. There is one agent per product (in our case, **BitDefender for File Servers**).

`NetProtect/Agents/FileServer/`

Contains the settings for the BitDefender for File Servers agent (they also include the File Server Service settings).

`NetProtect/Agents/FileServer/General/`

Contains the general settings for the BitDefender for File Servers agent.

`NetProtect/Agents/FileServer/General/IP/`

Stores the IP of the server on which BitDefender for File Servers is installed.

`NetProtect/Agents/FileServer/General/Lang/`

Stores the product language.

`NetProtect/Agents/FileServer/General/ServerName/`

Stores the name of the server on which BitDefender for File Servers is installed.

`NetProtect/Agents/FileServer/Key/`

Contains the settings regarding the license key.

`NetProtect/Agents/FileServer/Key/CRC/`

Stores the BitDefender for File Servers installation time or the registration time of the last valid key.

`NetProtect/Agents/FileServer/Key/Id/`

Stores the BitDefender for File Servers product id.

`NetProtect/Agents/FileServer/Key/IntermediateAlert/`

Three days before the product expires an alert is sent. The purpose of this key is to stop sending such alerts more than once in the last three days of the license period. If the alert was sent, then the key will have the `y` value.

`NetProtect/Agents/FileServer/Key/Key/`

Stores the currently registered product key.

`NetProtect/Agents/FileServer/Key/OldKey/`

Stores the previously registered valid key; when the product is first installed, `oldkey` is the same as `key`.

`NetProtect/Agents/FileServer/ODS/`

Contains the settings for the on-demand scan module.



- `NetProtect/Agents/FileServer/ODS/AV/`
Contains the settings for the on-demand scan antivirus.
- `NetProtect/Agents/FileServer/ODS/AV/FirstAction/`
Stores the first action to be taken on infected files for the on-demand scan antivirus.
- `NetProtect/Agents/FileServer/ODS/AV/SecondAction/`
Stores the second action to be taken on infected files for the on-demand scan antivirus if disinfection fails.
- `NetProtect/Agents/FileServer/ODS/Action/`
Stores the action to be taken on folders and files filtered in real time. There is a single action both for files and folders.
- `NetProtect/Agents/FileServer/ODS/Busy/`
The `Y` value indicates that an on-demand scan is in progress. Only one instance of the on-demand scanner is permitted.
- `NetProtect/Agents/FileServer/ODS/Cancel/`
If its value is `Y`, then the current on-demand scanning process will be cancelled.
- `NetProtect/Agents/FileServer/ODS/CurrentFile/`
Stores the path to the file currently scanned by the on-demand scan module.
- `NetProtect/Agents/FileServer/ODS/Extensions/`
Contains the settings for extension filtering in on-demand scanning.
- `NetProtect/Agents/FileServer/ODS/Extensions/Action/`
Stores the action to be taken for the on-demand extension filtering.
- `NetProtect/Agents/FileServer/ODS/Files/`
Contains the settings of the on-demand file filtering.
- `NetProtect/Agents/FileServer/ODS/Files/Number/`
Stores the number of user-specified files in on-demand file filtering.
- `NetProtect/Agents/FileServer/ODS/Files/Value<no>/Exclude/`
Its value is `Y` not to scan or `N` to scan the user-specified filename stored by the respective item.
- `NetProtect/Agents/FileServer/ODS/Files/Value<no>/Name/`
For each item `Value<no>`, this key stores a user-specified filename to be filtered on-demand.
- `NetProtect/Agents/FileServer/ODS/Folders/`
Contains the settings of the on-demand folder filtering.
- `NetProtect/Agents/FileServer/ODS/Folders/Number/`
Stores the number of user-specified folders in on-demand folder filtering.



- `NetProtect/Agents/FileServer/ODS/Folders/Value<no>/Exclude/`
Its value is **Y** not to scan or **N** to scan the user-specified folder name stored by the respective item.
- `NetProtect/Agents/FileServer/ODS/Folders/Value<no>/Name/`
For each item `Value<no>`, this key stores a user-specified folder name to be filtered on-demand.
- `NetProtect/Agents/FileServer/ODS/GenLog/`
If its value is **Y** a log is generated for the on-demand scan, while if it is **N** no log file is generated.
- `NetProtect/Agents/FileServer/ODS/LogInfected/`
If its value is **Y** only the infected files are logged in the on-demand scan report, while if it is **N** all scanned files are logged.
- `NetProtect/Agents/FileServer/ODS/MaxFileSize/`
Stores the maximum file size to be scanned on-demand.
- `NetProtect/Agents/FileServer/ODS/Path/`
Stores the path to the on-demand scan module.
- `NetProtect/Agents/FileServer/ODS/ReportPath/`
Stores the path where the on-demand scan report will be saved.
- `NetProtect/Agents/FileServer/RTP/`
Contains the settings for the real-time protection module.
- `NetProtect/Agents/FileServer/RTP/AV/`
Contains the settings for the real-time antivirus.
- `NetProtect/Agents/FileServer/RTP/AV/Deny/`
Sets the action to be taken on the infected files if the specified actions (e.g. **Disinfect / Delete**) fail. If its value is **Y** the access to infected files is denied.
- `NetProtect/Agents/FileServer/RTP/AV/FirstAction/`
Stores the first action to be taken on infected files in real-time scanning.
- `NetProtect/Agents/FileServer/RTP/AV/SecondAction/`
Stores the second action to be taken on infected files in real-time scanning if disinfection fails.
- `NetProtect/Agents/FileServer/RTP/Action/`
Stores the action to be taken on folders and files filtered in real time. There is a single action both for files and folders.
- `NetProtect/Agents/FileServer/RTP/Enabled/`
Stores the status of the real-time protection: **Y** for enabled or **N** for disabled.
- `NetProtect/Agents/FileServer/RTP/Extensions/`
Contains the settings for extension filtering in real-time scanning.



- `NetProtect/Agents/FileServer/RTP/Extensions/Action/`
Stores the action to be taken for real-time extension filtering.
- `NetProtect/Agents/FileServer/RTP/Files/`
Contains the settings of real-time file filtering.
- `NetProtect/Agents/FileServer/RTP/Files/Number/`
Stores the number of user-specified files in real-time file filtering.
- `NetProtect/Agents/FileServer/RTP/Files/Value<no>/Exclude/`
Its value is **Y** not to scan or **N** to scan the user-specified filename stored by the respective item.
- `NetProtect/Agents/FileServer/RTP/Files/Value<no>/Name/`
For each item `Value<no>`, this key stores a user-specified filename to be filtered in real time.
- `NetProtect/Agents/FileServer/RTP/Folders/`
Contains the settings of the real-time folder filtering.
- `NetProtect/Agents/FileServer/RTP/Folders/Number/`
Stores the number of user-specified folders in real-time folder filtering.
- `NetProtect/Agents/FileServer/RTP/Folders/Value<no>/Exclude/`
Its value is **Y** not to scan or **N** to scan the user-specified folder name stored by the respective item.
- `NetProtect/Agents/FileServer/RTP/Folders/Value<no>/Name/`
For each item `Value<no>`, this key stores a user-specified folder name to be filtered in real time.
- `NetProtect/Agents/FileServer/RTP/MaxFileSize/`
Stores the maximum file size to be scanned in real time.
- `NetProtect/Agents/FileServer/Status/`
Contains information about the status of the BitDefender for File Servers key. This information is not used to decide if a product is valid, but only to be shown in the management console.
- `NetProtect/Agents/FileServer/Status/ExpireTime/`
Stores the expiration time of the key.
- `NetProtect/Agents/FileServer/Status/KeyStatus/`
Stores the status of the key: valid, expired, invalid, etc.
- `NetProtect/Versions/`
Contains information about the versions of the most important product modules. This information can be seen in the **About** section from the management console.
- `NetProtect/Versions/BDFS/`
Contains information about the BitDefender for File Server service version.



`NetProtect/Versions/BDFS/Name/`

Stores the service name. This information can be seen in the **About** section from the management console.

`NetProtect/Versions/BDFS/Version/`

Stores the service version. This information can be seen in the **About** section from the management console.

`NetProtect/Versions/BDStat/`

Contains information about the BitDefender Statistics service version.

`NetProtect/Versions/BDStat/Name/`

Stores the service name. This information can be seen in the **About** section from the management console.

`NetProtect/Versions/BDStat/Version/`

Stores the service version. This information can be seen in the **About** section from the management console.

`NetProtect/Versions/FileServer/`

Contains information about the product version.

`NetProtect/Versions/FileServer/Name/`

Stores the product name. This information can be seen in the **About** section from the management console.

`NetProtect/Versions/FileServer/Version/`

Stores the product version. This information can be seen in the **About** section from the management console.



B. Appendix B - File List

In this appendix you can find a list of all product files along with their default installation path and the component they are part of. The files are sorted alphabetically to ease your search for a specific file.



Note

To find more information about what files are located in a certain directory, please check the *"File List"* (p. 44) section.

```
*.cvd
  \Program Files\Common Files\Softwin\AV\Plugins
  Scanning engine - plugins

*.ini
  \Program Files\Common Files\Softwin\Stats
  BitDefender Statistics Service

*.ivd
  \Program Files\Common Files\Softwin\AV\Plugins
  Scanning engine - plugins

*.rvd
  \Program Files\Common Files\Softwin\AV\Plugins
  Scanning engine - plugins

*.xmd
  \Program Files\Common Files\Softwin\AV\Plugins
  Scanning engine - plugins

antivirusstatus.png
  \Program Files\Common Files\Softwin\Console\HTMLS
  BitDefender GUI

avxdisk.dll
  \Program Files\Common Files\Softwin\AV
  Scanning engine

avxs.dll
  \Program Files\Common Files\Softwin\AV
  Scanning engine

avxt.dll
  \Program Files\Common Files\Softwin\AV
  Scanning engine
```



```
bar.png
  \Program Files\Common Files\Softwin\Console\HTMLS
  BitDefender GUI
bar_left.png
  \Program Files\Common Files\Softwin\Console\HTMLS
  BitDefender GUI
bar_right.png
  \Program Files\Common Files\Softwin\Console\HTMLS
  BitDefender GUI
bd_left.bmp
  \Program Files\Common Files\Softwin\Console\HTMLS
  BitDefender GUI
bd_middle.bmp
  \Program Files\Common Files\Softwin\Console\HTMLS
  BitDefender GUI
bd_right.bmp
  \Program Files\Common Files\Softwin\Console\HTMLS
  BitDefender GUI
bd.log
  \Program files\Common Files\Softwin
  BitDefender Logging Service
bdc.exe
  \Program Files\Common Files\Softwin\AV
  Scanning engine
bdc.ini
  \Program Files\Common Files\Softwin\AV
  Scanning engine
bdch.dll
  \Program Files\Softwin\BitDefender for File Servers
  BitDefender Error Report Wizard
bdch.ini
  \Program Files\Softwin\BitDefender for File Servers
  BitDefender Error Report Wizard
bdconsole.dll
  \Program Files\Common Files\Softwin\Console
```



BitDefender GUI

bdconsole.exe
 \Program Files\Common Files\Softwin\Console

BitDefender GUI

BDConsoleLang.dll
 \Program Files\Common Files\Softwin\Console

BitDefender GUI

bdcore.dll
 \Program Files\Common Files\Softwin\AV

Scanning engine

bdfs.exe
 \Program Files\Softwin\BitDefender for File Servers

On-Access Scan Module

bdfslang.dll
 \Program Files\Softwin\BitDefender for File Servers\Lang

On-Access Scan Module

bdlived.exe
 \Program Files\Common Files\Softwin

BitDefender Live Update Service

bdlivedlang.dll
 \Program Files\Common Files\Softwin\Lang

BitDefender Live Update Service

bdlogd.exe
 \Program files\Common Files\Softwin

BitDefender Logging Service

bdlogdlang.dll
 \Program files\Common Files\Softwin\Lang

BitDefender Logging Service

bdregsvr2.exe
 \Program Files\Common Files\Softwin\BDReg

BitDefender Registry

bdregsvr2.pem
 \Program Files\Common Files\Softwin\BDReg

BitDefender Registry



bdscand.exe
 \Program Files\Common Files\Softwin
 BitDefender Scanning Service

bdscandlang.dll
 \Program Files\Common Files\Softwin\Lang
 BitDefender Scanning Service

bdsetup.exe
 \Program Files\Common Files\Softwin
 BitDefender Setup

BDScheduler.exe
 \Program Files\Common Files\Softwin
 BitDefender Scheduler Service

BDSchedulerLang.dll
 \Program Files\Common Files\Softwin\Lang
 BitDefender Scheduler Service

BDStat.exe
 \Program Files\Common Files\Softwin\Stats
 BitDefender Statistics Service

BDStatLang.dll
 \Program Files\Common Files\Softwin\Stats\Lang
 BitDefender Statistics Service

bdsubmit.dll
 \Program Files\Softwin\BitDefender for File Servers
 BitDefender Error Report Wizard

bdsubmit.exe
 \Program Files\Softwin\BitDefender for File Servers
 BitDefender Error Report Wizard

bdsubmit.ini
 \Program Files\Softwin\BitDefender for File Servers
 BitDefender Error Report Wizard

bdupd.dll
 \Program Files\Common Files\Softwin\AV
 Scanning engine



```
bdupdconfig.exe
  \Program Files\Softwin\BitDefender Enterprise Manager\BitDefender
  Update Server
Update Server

bdupdsvr.exe
  \Program Files\Softwin\BitDefender Enterprise Manager\BitDefender
  Update Server
Update Server

BDUPDSVR.ini
  \Program Files\Softwin\BitDefender Enterprise Manager\BitDefender
  Update Server
Update Server

bitdefender.msc
  \Program Files\Common Files\Softwin\Console
BitDefender GUI

button1.bmp
  \Program Files\Common Files\Softwin\Console\HTMLS
BitDefender GUI

button2.bmp
  \Program Files\Common Files\Softwin\Console\HTMLS
BitDefender GUI

context_np.bmp
  \Program Files\Common Files\Softwin\BitDefender Local Manager\Task
  Templates
BitDefender Local Manager

dot.png
  \Program Files\Common Files\Softwin\Console\HTMLS
BitDefender GUI

down.gif
  \Program Files\Common Files\Softwin\Console\HTMLS
BitDefender GUI

down.png
  \Program Files\Common Files\Softwin\Console\HTMLS
BitDefender GUI

down_left.png
  \Program Files\Common Files\Softwin\Console\HTMLS
```



BitDefender GUI

down_right.png
 \Program Files\Common Files\Softwin\Console\HTMLS

BitDefender GUI

ErrorMsg.ptt
 \Program files\Common Files\Softwin\BDLog\Templates
 \Program files\Common Files\Softwin\BDLog\Nettemplates

BitDefender Logging Service - alert templates

filelog.npl
 \Program files\Common Files\Softwin\BDLog

BitDefender Logging Service

fileloglang.dll
 \Program files\Common Files\Softwin\BDLog\Lang

BitDefender Logging Service

FileServerMsg.ptt
 \Program files\Common Files\Softwin\BDLog\Templates
 \Program files\Common Files\Softwin\BDLog\Nettemplates

BitDefender Logging Service - alert templates

filespy.sys
 \Program Files\Softwin\BitDefender for File Servers

BitDefender for File Server Driver

filespy9x.dll
 \Program Files\Softwin\BitDefender for File Servers

BitDefender for File Server Driver

fs_config.tsi
 \Program Files\Common Files\Softwin\BitDefender Local Manager\Task
 Templates

BitDefender Local Manager

fs_stats.tsi
 \Program Files\Common Files\Softwin\BitDefender Local Manager\Task
 Templates

BitDefender Local Manager

fsmon.dll
 \Program Files\Softwin\BitDefender for File Servers

BitDefender for File Server Driver



fsodlang.dll
 \Program Files\Softwin\BitDefender for File Servers\Lang
On-Demand Scan Module

fsondemand.exe
 \Program Files\Softwin\BitDefender for File Servers
On-Demand Scan Module

getfile.dll
 \Program Files\Softwin\BitDefender for File Servers
Authentication Module

http.exe
 \Program files\Common Files\Softwin\BitDefender HTTP Server
Update Server

httpconfig.xml
 \Program files\Common Files\Softwin\BitDefender HTTP Server
Update Server

httpgetfile.dll
 \Program Files\Softwin\BitDefender Enterprise Manager\BitDefender
 Update Server
Update Server

iconv.dll
 \Program Files\Common Files\Softwin\CFilter
Content Filter Module

index.html
 \Program Files\Common Files\Softwin\Console\HTMLS
BitDefender GUI

InfoMsg.ptt
 \Program files\Common Files\Softwin\BDLog\Templates
 \Program files\Common Files\Softwin\BDLog\Nettemplates
BitDefender Logging Service - alert templates

KeyHasExpiredMsg.ptt
 \Program files\Common Files\Softwin\BDLog\Templates
 \Program files\Common Files\Softwin\BDLog\Nettemplates
BitDefender Logging Service - alert templates

KeyWillExpireMsg.ptt
 \Program files\Common Files\Softwin\BDLog\Templates



```
\Program files\Common Files\Softwin\BDLog\Nettemplates
  BitDefender Logging Service - alert templates
label.dat
  BitDefender Live Update Service
libfn.dll
  \Program Files\Common Files\Softwin\AV
  Scanning engine
mfc70.dll
  \System32
  Auxiliary files
mfc71.dll
  \System32
  Auxiliary files
mfc71u.dll
  \System32
  Auxiliary files
mn_smtp.npl
  \Program files\Common Files\Softwin\BDLog
  BitDefender Logging Service
msvcp70.dll
  \System32
  Auxiliary files
msvcp71.dll
  \System32
  Auxiliary files
msvcr70.dll
  \System32
  Auxiliary files
msvcr71.dll
  \System32
  Auxiliary files
nn-winnt.npl
  \Program files\Common Files\Softwin\BDLog
  BitDefender Logging Service
```



normal_np.bmp
 \Program Files\Common Files\Softwin\BitDefender Local Manager\Task
 Templates
BitDefender Local Manager

np_stats.tsi
 \Program Files\Common Files\Softwin\BitDefender Local Manager\Task
 Templates
BitDefender Local Manager

np_status.tsi
 \Program Files\Common Files\Softwin\BitDefender Local Manager\Task
 Templates
BitDefender Local Manager

npemclient.exe
 \Program Files\Common Files\Softwin
BitDefender Local Manager

NPFilter.dll
 \Program Files\Common Files\Softwin\CFilter
Content Filter Module

npfs.chm
 \Program Files\Softwin\BitDefender for File Servers
Product Documentation

OnDemandMsg.ptt
 \Program files\Common Files\Softwin\BDLog\Templates
 \Program files\Common Files\Softwin\BDLog\Nettemplates
BitDefender Logging Service - alert templates

plugins.htm
 \Program Files\Common Files\Softwin\AV
Scanning engine

product update.html
 \Program Files\Common Files\Softwin\Console\HTMLS
BitDefender GUI

products.dat
 \Program Files\Common Files\Softwin\BitDefender Local Manager
BitDefender Local Manager



```
rtvr.npl
  \Program files\Common Files\Softwin\BDLog
  BitDefender Logging Service

run_fs_scan.tsi
  \Program Files\Common Files\Softwin\BitDefender Local Manager\Task
  Templates
  BitDefender Local Manager

run_update.tsi
  \Program Files\Common Files\Softwin\BitDefender Local Manager\Task
  Templates
  BitDefender Local Manager

serverstatus.png
  \Program Files\Common Files\Softwin\Console\HTMLS
  BitDefender GUI

small_np.bmp
  \Program Files\Common Files\Softwin\BitDefender Local Manager\Task
  Templates
  BitDefender Local Manager

status.html
  \Program Files\Common Files\Softwin\Console\HTMLS
  BitDefender GUI

top.gif
  \Program Files\Common Files\Softwin\Console\HTMLS
  BitDefender GUI

top.png
  \Program Files\Common Files\Softwin\Console\HTMLS
  BitDefender GUI

up.png
  \Program Files\Common Files\Softwin\Console\HTMLS
  BitDefender GUI

up_left.png
  \Program Files\Common Files\Softwin\Console\HTMLS
  BitDefender GUI

up_right.png
  \Program Files\Common Files\Softwin\Console\HTMLS
```



BitDefender GUI

updatestatus.png
 \Program Files\Common Files\Softwin\Console\HTMLS

BitDefender GUI

updprod.ini
 \Program Files\Softwin\BitDefender Enterprise Manager\BitDefender
 Update Server

Update Server

WarningMsg.ptt
 \Program files\Common Files\Softwin\BDLog\Templates
 \Program files\Common Files\Softwin\BDLog\Nettemplates

BitDefender Logging Service - alert templates

xcomm.dll
 \System32

BitDefender Local Manager

xcommsvr.exe
 \Program files\Common Files\Softwin\BitDefender Communicator

BitDefender Communicator

xdb.xml
 \Program Files\Common Files\Softwin\BDReg

BitDefender Registry

xgate.dll
 \Program files\Common Files\Softwin\BitDefender Communicator

BitDefender Communicator

xreglib.dll
 \System32

BitDefender Registry

versions.dat
 BitDefender Live Update Service



C. Appendix C - Services

In this appendix you can find all the BitDefender services and their description.

Note



To find more information about the BitDefender Services and the way they work, please check the *“Technical Diagram - In-depth View”* (p. 8) section.

BitDefender for File Servers Service - `bdfs.exe`

Ensures that accessed files are scanned.

It receives the accessed file from the BitDefender driver and sends it to the Content Filter to see if it should be scanned or not. If the Content Filter response is SCAN, it will send the file to the Scanning Service to be scanned. Based on the scan result, an appropriate action will be taken by the service and the **Allow / Deny access** response will be sent to the driver.

BitDefender Live Update Service - `bdlived.exe`

Keeps BitDefender up to date. The service searches for updates:

- **automatically**, based on the settings from the registry keys. It takes the proxy settings and the update interval and location from `xdb.xml`, but it computes by itself when to do the next check for updates.
- **manually**, when the user requests an update by clicking **Scan now** or when the Scheduler Service indicates that an update must be performed.

If engine updates are available, it automatically downloads the files and replaces the old ones from the disk. If a product update is available, it notifies the user about the new version and the download link.

BitDefender Logging Service - `bdlogd.exe`

Receives the information sent by the agent components (the On-access and On-demand Scan modules) and manages it using four plugins:

- **filelog.npl** - logs the information in the log file. The default log file is: `C:\Program Files\Common Files\Softwin\BDLog\bd.log`.
- **mn-smtp.npl** - sends mail alerts to the specified receivers.
- **winnt.npl** - sends net send alerts to the specified receivers.
- **rtvr.npl** - sends reports to the BitDefender Lab regarding real-time virus activity on the local machine.

BitDefender Registry Service - `bdregsvr2.exe`, `bdregsvr2.pem`, `xdb.xml`

Manages the BitDefender settings. Other components send requests to this service to read / write settings from / to the registry keys. Therefore, all BitDefender components depend on it.

For example, when a component is registered, it sends its default settings to the BitDefender Registry Service, which writes them in the `xdb.xml` file.



BitDefender Scanning Service - `bdscand.exe`

Scans the files received from the On-access and On-demand scan modules, using the antivirus engines and plugins.

BitDefender Scheduler Service - `BDScheduler.exe`

Schedules scan and update tasks to be executed at a later time.

BitDefender Statistics Service - `BDstat.exe`, `*ini` files

Manages the BitDefender statistics based on the information received from the agent components (the On-access and On-demand Scan modules).