Bitdefender

Bitdefender Security for LabTech

PLUGIN USER GUIDE

Bitdefender Security for LabTech Plugin User Guide

Publication date 2018.02.13

Legal Notice

Table of Contents

1. About 1
2. Installation Requirements 2
2.1. Bitdefender Plugin 2
2.2. Bitdefender Agent 2
3. Plugin Installation 5
3.1. Installing the Plugin 5
3.2. Updating the Plugin 7
4. Getting Started 8
5. Configuring the Plugin 35
5.1. Licensing 11
5.2. Security 13
5.3. Alerts 14
6. Agent Deployment 15
6.1. Preparing for Installation 15
6.2. Deploying the Agent 16
6.2.1. Auto Deployment 16
6.2.2. Manual Deployment 17
7. Policies 19
7.1. Managing Policies 19
7.1.1. Creating Policies 19
7.1.2. Editing Policies 20
7.1.3. Assigning Policies 20
7.1.4. Deleting Policies 21
7.2. Policy Settings 21
7.2.1. General 21
7.2.2. Anti-Malware 23
8. Quarantine 28
8.1. Exploring the Quarantine 28
8.2. Restoring Quarantined Files 29
8.3. Deleting Quarantined Files 30
9. Reports 31
9.1. Using Reports 31
9.2. Report Types 32
10. Audit Logs 35
11. Uninstallation 37
11.1. Uninstalling the Agent 37
11.2. Uninstalling the Plugin 37
12. Getting Help 39

12.1. Bitdefender Support Center 39
12.2. Asking for Assistance 40
12.3. Contact Information 40

1. ABOUT

Bitdefender Security for LabTech provides enterprise-class antimalware services integrated with the LabTech systems for deploying, monitoring, and interacting with the Bitdefender Endpoint Security agent, an enterprise-class award-winning antimalware solution.

LabTech administrators can use the plugin to remotely install the Bitdefender Endpoint Security agent, manage licensing of the agent across their organizations, assign custom policies to organizations, machine groups or individual machines, and initiate different types of malware scans. Malware detection data are collected and can be used to generate reports and alerts. The plugin significantly enhances LabTech administrators' ability to manage large deployments of Bitdefender agents.

2. INSTALLATION REQUIREMENTS

2.1. Bitdefender Plugin

The Bitdefender Plugin has been designed with the following assumptions and requirements:

Software Requirements

- The plugin can be installed only on **LabTech 10.5 and 11** systems. Based on this requirement, the installer informs you if it is able to proceed.
- The plugin supports only Bitdefender Endpoint Security version 5.xx as security agent.

Hardware Requirements

To be able to install and run, the Bitdefender Plugin requires additional server hardware resources as follows:

- RAM memory: 2 GB
- Free HDD space: 2 GB

If your LabTech server runs on a virtual machine, additional CPU cores can help with performance, particularly with IIS.

2.2. Bitdefender Agent

Supported Operating Systems

Bitdefender Endpoint Security protects the following operating systems:

Workstation operating systems

- Windows 10 TH2 (*)
- Windows 10 (*)
- Windows 8.1
- Windows 8
- Windows 7
- Windows Vista with Service Pack 1

- Windows XP with Service Pack 2 64 bit
- Windows XP with Service Pack 3

(*) Windows 10 support is available starting with Endpoint Security version 5.3.23.704.

Tablet and embedded operating systems

- Windows Embedded 8.1 Industry
- Windows Embedded 8 Standard
- Windows Embedded Standard 7
- Windows Embedded Compact 7
- Windows Embedded POSReady 7
- Windows Embedded Enterprise 7
- Windows Embedded POSReady 2009
- Windows Embedded Standard 2009
- Windows XP Embedded with Service Pack 2 (*)
- Windows XP Tablet PC Edition (*)

(*) Specific operating system modules must be installed for Endpoint Security to work.

Server operating systems

- Windows Server 2012 R2
- Windows Server 2012
- Windows Small Business Server (SBS) 2011
- Windows Small Business Server (SBS) 2008
- Windows Server 2008 R2
- Windows Server 2008
- Windows Small Business Server (SBS) 2003
- Windows Server 2003 R2
- Windows Server 2003 with Service Pack 1
- Windows Home Server

Additional Software Requirements

- .NET Framework 4.0
- LabTech agent

Hardware Requirements

Processor

Endpoint Security requires Intel® Pentium compatible processor as follows:

- For Workstation Operating Systems:
  - 1 GHz or faster for Microsoft Windows XP SP3, Windows XP SP2 64 bit and Windows 7 Enterprise (32 and 64 bit)
  - 2 GHz or faster for Microsoft Windows Vista SP1 or higher (32 and 64 bit), Microsoft Windows 7 (32 and 64 bit), Microsoft Windows 7 SP1 (32 and 64bit), Windows 8, Windows 10 and Windows 10 TH2
  - 800 MHZ or faster for Microsoft Windows Embedded Standard 7 SP1, Microsoft Windows POSReady 7, Microsoft Windows POSReady 2009, Microsoft Windows Embedded Standard 2009, Microsoft Windows XP Embedded with Service Pack 2, Microsoft Windows XP Tablet PC Edition
- For Server Operating Systems:
  - Minimum: 2.4 GHz single-core CPU
  - Recommended: 1.86 GHz or faster Intel Xeon multi-core CPU

Free RAM memory

512 MB minimum, 1 GB recommended

HDD space

1.5 GB of free hard-disk space

3. PLUGIN INSTALLATION

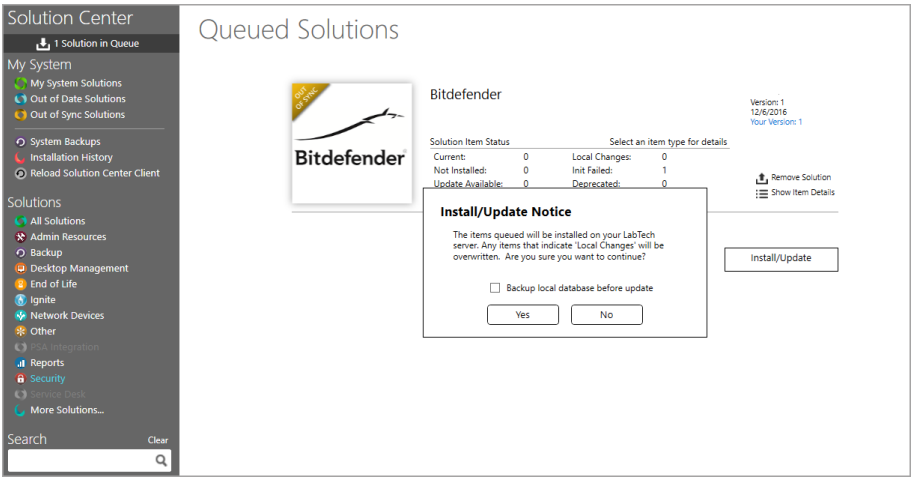
LabTech Control Center provides you a simple and unitary way to install and update the Bitdefender Plugin.

3.1. Installing the Plugin

To install the Bitdefender Plugin:

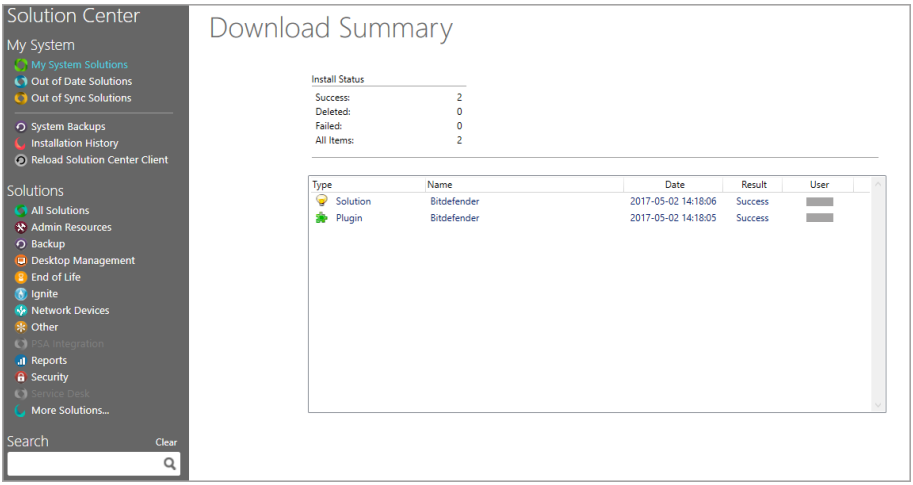
1. Perform a System Backup.
2. Open LabTech Control Center and access Solution Center.
3. In the left-side menu, go to the **Solutions** list and click **Security**.
4. Look for the Bitdefender icon in the **Security Solutions** right-side panel and select it. A new window will open. (Alternatively, you can use the **Search** field on the left-side to find Bitdefender.)
5. Click the **Queue** button to prepare the Bitdefender Plugin for installation, then click **Yes** in the **Terms of Service** window to confirm your action.
6. Back in the **Security Solutions** panel, the Bitdefender icon displays the **In Queue** status. Select it again and a new page will open.

7. In the **Queued Solutions** page, click the **Install/Update** button.
8. You must confirm the action in the **Install/Update Notice** window. Select the **Backup local database before update** check box if you want to do that and click **Yes**.



9. The installation process begins. When it is completed, click the **Finished** button.

To review the installation status, go to **My System Solutions**. The **Download Summary** page will provide you specific details, such as type of the package, name, date, installation result and user.



3.2. Updating the Plugin

When a new version of the Bitdefender Plugin is release, it will be available in the LabTech Solution Center. The update will be performed exclusively via Solution Center following the same steps as for installation. For more information, refer to Installing the Plugin.

4. GETTING STARTED

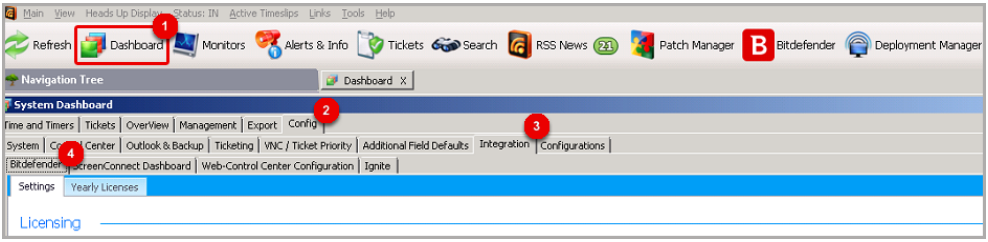
The Bitdefender Plugin adds new tabs to your LabTech Control Center screens, allowing you to configure product settings, setup licensing information and review logging and reporting data. Please find hereinafter a brief overview of these tabs.

System Dashboard Screen

The **Bitdefender** tab of the **System Dashboard** screen is primarily used for configuring settings such as **Licensing** and **Alerting**.

To access the Bitdefender configuration tab:

1. From the LabTech Toolbar, click the **Dashboard** button.
2. In the **System Dahboard** screen, select the **Config > Integration > Bitdefender** tab.



Plugin Dashboard Screen

The Bitdefender Plugin Dashboard is the main screen you will use for daily maintenance or review. From this dashboard you can quickly view computer threat information, manage policies and audit plugin usage.

You can easily access the Plugin Dashboard from the LabTech Toolbar by clicking the **Bitdefender** button.

The Plugin Dashboard consists of these tabs:

- **Main** tab, informing you of the network protection status through various charts and statistics related to malware detected, blocked applications and product updates.
- **Policies** tab, allowing you to create, edit, clone, delete and assign policies to computers protected by Bitdefender.
- **Quarantine** tab, displaying all files currently in quarantine and allowing you to restore or remove them from the affected computer.
- **Audit** tab, showing all user actions related to Bitdefender installation and policies.
- **Help** tab, showing you the present User Guide.

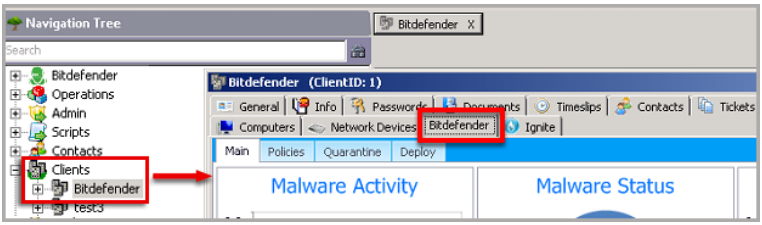
Client Screen

The Bitdefender tab in the Client screen allows you to view centralized statistics about security issues of an organization and to manage Bitdefender agent deployment, antimalware policies and quarantined files.

The Bitdefender tab consists of several other tabs, similar to the ones in Plugin Dashboard, except they are limited to a specific client. Also, the Client screen has an additional **Deploy** tab, allowing you to enable Auto-deployment and issue manual deployment commands such as Installs and Uninstalls.

To access the Bitdefender tab for a specific client:

1. From the LabTech Nagivation Tree, expand the **Clients** group.
2. Double-click a client's name to open the corresponding Client screen.
3. Select the **Bitdefender** tab.



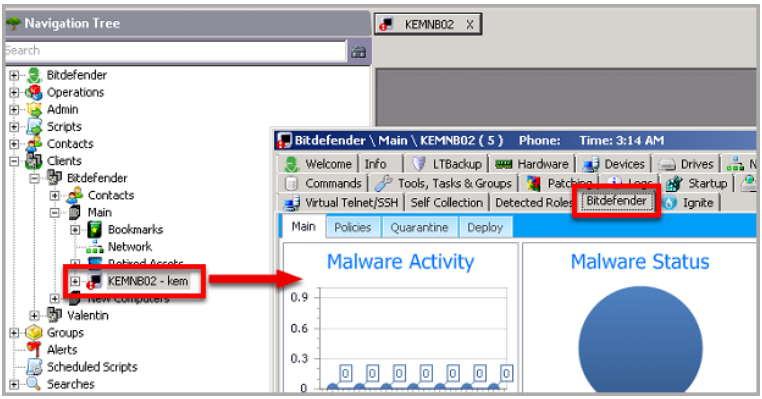
Computer Screen

The Bitdefender tab on the Computer screen shows security issues detected by the Bitdefender agent on the remote computer, allows you to enable or disable Auto-deployment, to issue manual deployment commands, such as Installs and

Uninstalls, and to assign existing Bitdefender policies. The tabs are similar to the ones in the Client screen, except they only apply to that specific computer.

To access the Bitdefender tab for a specific computer:

1. From the Nagivation Tree, expand **Clients** > client > location.
2. Double-click the computer hostname to open the corresponding Computer screen.
3. Select the **Bitdefender** tab.



5. CONFIGURING THE PLUGIN

Initially, the plugin runs using a default configuration. The settings allow you to register Security for ConnectWise, to enhance the plugin security and to receive alerts related to license usage, outdated computers or malware outbreaks in your Client networks.

To configure the plugin:

1. From the LabTech Toolbar, click the **Dashboard** button.
2. Navigate to the **Config > Integration > Bitdefender** tab.
3. Change the plugin settings as needed. Settings are organized under the following categories:
   - Licensing
   - Security
   - Alerting
4. Click **Save**.

5.1. Licensing

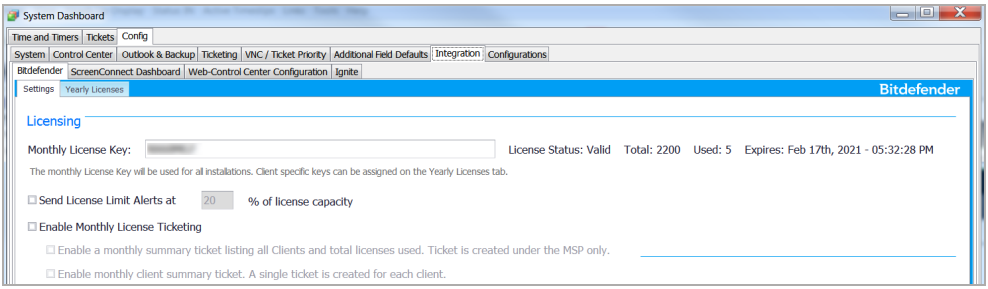
You can use Security for ConnectWise as trial for 30 days. During this time you can try all features the service provides. When the trial expires, you must enter a valid license key, otherwise updates and antimalware protection become unavailable.

Security for ConnectWise uses by default a monthly license, available for all agent installations.

Important
If you are unsure what a monthly license is or if you do not have a monthly license key, please contact us before using the plugin.

To register Security for ConnectWise, enter the license key in the **Monthly License Key** field. You will then be able to view license details such as status, usage and validity at the right side of the field. After the key is validated, the agents automatically receive the license information and endpoints are being protected.

Though you can add a license key at any time, our recommendation is to add it before agent deployment.

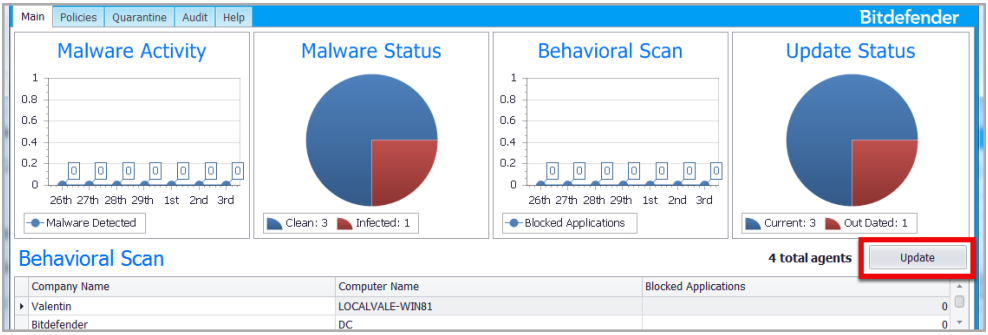


Note

You can also notice the plugin contains the **Yearly Licenses** tab. Bitdefender does not support yearly per client licensing system yet. The license key you received will not work in this tab.

In the event that the license is not applied on specific endpoints, you can manually trigger the license deployment by clicking the **Update** button in the **Main** tab of the following screens:

- Client screen, to license all endpoints of an organization.
- Computer screen, to license a specific endpoint.



Once registered, you can easily control license usage by choosing to receive alerts and reports. These are the available options:

Option	Description
Send License Limit Alerts	Enable this option to receive email alerts when your license reaches the threshold provided in the associated field. This way, you know when you need to extend the license to allow more agent installations.  **Warning** You must enter a value greater or equal to 10. **DEFAULT:** Disabled
Enable Monthly License Usage Ticketing	When enabled, you receive on email either a single ticket with all client information or individual tickets per client, depending on the selection made. **DEFAULT:** Disabled

5.2. Security

This section contains the following security related settings:

Setting	Description
Restrict Settings and Policy to Super Admin	Enable this option to allow only Super Admins or users with higher rights in LabTech to access the **Settings** or **Policy** tabs from System and Plugin Dashboards. **DEFAULT:** Disabled
Bitdefender Update URL	Bitdefender uses this URL to send agent and signature updates. Unless you have an alternative Bitdefender update server at hand, you will not need to edit this field. **DEFAULT:** `upgrade.bitdefender.com`

5.3. Alerts

Alerts are email notifications to inform you of critical security events such as malware outbreaks. These are the available alerts:

Alert	Description
Agent out-of-date alert threshold	When enabled, allows you to define the number of days after which to be alerted for an outdated agent. **DEFAULT:** Disabled
Malware Outbreak Threshold	When enabled, allows you to define the infected endpoints percentage that will trigger an alert, if exceeded. **Warning** You must enter a value greater or equal to 10. **DEFAULT:** Disabled

6. AGENT DEPLOYMENT

To protect the computers of your client networks, you must install the security agent on each of them. Besides managing protection on the remote computer, the security agent also communicates with the Bitdefender plugin to receive the administrative commands and to send the results of its actions.

Important
Bitdefender agent deployment is to be handled by the plugin as the log and scan history require certain settings to be collected correctly.

There are two deployment scenarios:

Bitdefender agent is not installed.
The LabTech installation script will detect that Bitdefender agent is not installed, it will install `LTBitdefenderService` first and then it will deploy the software. `LTBitdefenderService` connects the current installation to LabTech.

Bitdefender agent is already installed.
The LabTech installation script will detect the Bitdefender agent on the machine and it will just install `LTBitdefenderService`.

6.1. Preparing for Installation

Before proceeding with the Bitdefender agent deployment:

1. Make sure that the remote computers meet the installation requirements.
2. Each target computer must allow remote connection. Thus, the `admin$` administrative share must be enabled.
3. Uninstall (not just disable) any existing antimalware, firewall or Internet security software from target endpoints. Running the security agent simultaneously with other security software on an endpoint may affect their operation and cause major problems with the system.

   Many of the security programs that are incompatible with Bitdefender agent are automatically detected and removed at installation time. To learn more and to check the list of detected security software, refer to this Bitdefender KB article.
4. Temporarily turn off User Account Control on all computers running Windows operating systems that include this security feature (Windows Vista, Windows

7, Windows Server 2008 etc.). If the computers are in a domain, you can use a group policy to turn off User Account Control remotely.

Best Practice

The security agent automatically performs an initial security assessment on the target endpoints once the installation has finished. Therefore, it is recommended to use a phased deployment approach. This is to help offload the potential high number of threats reported during the initial scan, reducing the possibility of performance problems with IIS on your LabTech server.

When deploying the Bitdefender agent, you should consider the following guidelines:

1. Run maximum 200 installations at a time.

   For clients with more than 200 machines in LabTech, enable auto deployment on a location at a time. You can re-enable auto deployment on all locations after the initial deployment is complete.

2. Allow 12-24 hours (depending on server resource usage) for the Bitdefender agent to fully detect and report all initial threats.

6.2. Deploying the Agent

6.2.1. Auto Deployment

Use auto deployment to install the Bitdefender agent with minimum effort on your side, regardless of the network size. The plugin detects any new computer in the LabTech system and automatically installs the Bitdefender agent on it.

Note
Auto deployment is disabled by default.

To enable or disable auto deployment in a specific client's network:

1. Expand the **Clients** group in the **Navigation Tree**.
2. Double-click the client's name to open the Client screen.
3. Select the **Bitdefender > Deploy** tab.
4. Click the **Auto-deployment** button to switch auto deployment ON or OFF.

To manage auto deployment only for a specific computer, go to the **Deploy** tab of the Computer screen.

There are certain situations in which you may want to exclude some computers from auto deployment. For example, you have a group of servers running critical services and you want to have control when they reboot.

To exclude an entire location from auto deployment:

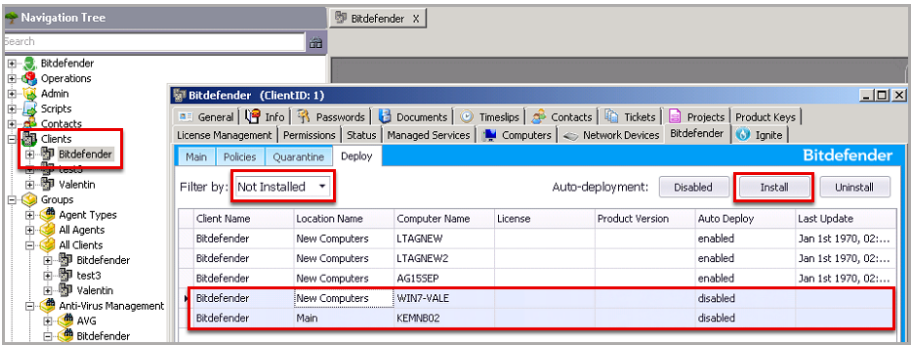
1. Expand the **Clients** group in the **Navigation Tree**.
2. Double-click the selected location to open the Location screen.
3. Select the **Bitdefender** tab.
4. Select the **Exclude Location from AutoDeploy** check box.
5. Click **Save**. Bitdefender Plugin will ignore any new computer added to this location and the Bitdefender agent will not install on it.

6.2.2. Manual Deployment

You can manually install the Bitdefender agent on one or more computers at a time.

To deploy the Bitdefender agent on several computers within an organization:

1. Expand the **Clients** group in the **Navigation Tree**.
2. Open the Client screen by clicking the organization's name.
3. Select the **Bitdefender > Deploy** tab.
4. From the **Filter**menu at the upper left side of the tab, select **Not Installed** to filter the unprotected computers.
5. Select the computers on which you want to deploy the security agent.
6. Click the **Install** button at the upper right side of the tab. A pop-up window will confirm the operation. If the installation fails, a ticket will be generated.



To install the Bitdefender agent on a specific computer:

1. From the **Navigation Tree**, expand the **Clients > client > location** group that contains the computer.
2. Open the Computer screen by clicking the computer name.
3. Select the **Bitdefender > Deploy** tab.
4. Click the **Install** button at the upper right side of the tab. A pop-up window will confirm the operation. If the installation fails, a ticket will be generated.

7. POLICIES

Once installed, the Bitdefender protection can be configured and managed from LabTech Control Center using security policies. A policy specifies the security settings to be applied on target computers.

Immediately after installation, security agents are assigned with the default policy, which is preconfigured with the recommended protection settings. You cannot modify or delete the default policy. You can only view its settings when creating a new policy.

7.1. Managing Policies

You can view and manage policies in the **Bitdefender > Policies** tab available in any of these screens:

- Plugin Dashboard screen
- Client screen
- Computer screen

Each screen displays all policies, but restricts access to targets according to screens hierarchy. Thus, in the Client screen you can view and assign policies only to computers belonging to the selected client.

Existing policies are displayed in the table. For each policy, you can view:

- Policy name.
- User who created the policy.
- Date and time when the policy was last modified.

7.1.1. Creating Policies

You can create new policies starting from the default settings or using a clone of an existing custom policy.

To create a new policy:

1. Click the **New** button at the upper side of the **Policies** tab.
2. Configure the policy settings as needed.
   For detailed information, refer to "Policy Settings" (p. 21).
3. Click **Save**.

To create a policy from another one:

1. Select the policy you want to use as template in the Policies table.
2. Click the **Clone** button at the upper side of the **Policies** tab.
3. Configure the policy settings as needed.
   For detailed information, refer to "Policy Settings" (p. 21).
4. Click **Save**.

7.1.2. Editing Policies

You can change the settings of an existing policy anytime you want.

To edit a custom policy:

1. Select the policy in the Policies table.
2. Click the **Edit** button at the upper side of the **Policies** tab.
3. Configure the policy settings as needed.
   For detailed information, refer to "Policy Settings" (p. 21).
4. Click **Save**.

7.1.3. Assigning Policies

All computers are initially assigned with the default policy. The default policy is always included with the plugin and will be used if no other policy is assigned to a computer. A computer can have only one policy assigned to it at a time.

To assign a policy:

1. Click the **Assign** button at the upper side of the **Policies** tab.
2. Choose the appropriate targets view in accordance with your needs:
   - Click the **Clients** button if you want to assign the policy to the entire organization.

- Click the **Computers** button if you want to assign the policy to specific computers.

3. Select the target from the table.
4. Choose an available policy from the drop-down menu and then click **Set Policy**.

   Policies are pushed to target computers within minutes after changing the policy assignments or after modifying the policy settings. If a computer is not online, settings will be applied as soon as it gets back online.

To revert to the default policy, select your target and click the **Clear Policy** button.

7.1.4. Deleting Policies

If you no longer need a policy, you can delete it. Once the policy is deleted, the computers to which it used to apply will be assigned the policy of the parent group. If no other policy applies, the default policy will be enforced eventually.

To delete a policy, select it in the Policies table and click the **Delete** button at the upper side of the **Policies** tab.

7.2. Policy Settings

The policy settings are organized under the following categories:

- General
- Anti-Malware

7.2.1. General

General settings help you view policy properties, rename it and manage notifications display options, logs and update preferences for the target computers. The settings are organized into the following tabs:

- Settings
- Display
- Advanced
- Update

Settings

The **Settings** tab contains the general policy details:

- Policy name
- User who created the policy
- Date and time when the policy was created
- Date and time when the policy was last modified

Display

Option	Description
Enter Silent Mode	Silent Mode is designed to help you easily disable user interaction with the Bitdefender agent. **DEFAULT:** Disabled
Show icon in notification area	The icon in the Notification area (system tray) informs users on their protection status by changing its appearance and displaying a corresponding notification pop-up. Additionally, users can right-click it to quickly open the agent main window or the **About** window. Opening the **About** window automatically updates the product and engines when outdated. **DEFAULT:** Enabled
Display notification pop-ups	The notification pop-ups inform users about important security events such as the detection of malware and the action taken. **DEFAULT:** Disabled
Display alert pop-ups	Different from notification pop-ups, alert pop-ups prompt users for action. If you choose not to display alert pop-ups, the security agent automatically takes the recommended action. **DEFAULT:** Disabled
Status Alerts	Users determine when their computer has security configuration issues or other security risks, based on status alerts. For example, users can view whenever there is a problem related to their antimalware protection, such as: On-Access scanning module is disabled or a full system scan is overdue. **DEFAULT:** Custom

Advanced

Option	Description
Remove events older than (days)	Shows the number of days after which the security agent deletes the events log from the target computer. **DEFAULT:** 30
Submit crash reports to Bitdefender	When enabled, the agent sends reports to Bitdefender Labs for analysis if it crashes. The reports will help Bitdefender engineers find out what caused the problem and prevent it from occurring again. No personal information will be sent. **DEFAULT:** Enabled

Update

Option	Description
Signature Update	When enabled, the agent automatically checks for signature updates every hour. Automatic updates are performed silently in the background. **DEFAULT:** Enabled
Recurrence	You can change the automatic update recurrence by selecting a different option from the menu and configuring the subsequent fields according to your needs. **DEFAULT:** Hourly

7.2.2. Anti-Malware

The Anti-malware module protects the system against all kinds of malware threats (viruses, Trojans, spyware, rootkits, adware and so on). The protection is divided in two categories:

- On-access scanning: prevents new malware threats from entering the system.
- On-demand scanning: allows detecting and removing malware already residing in the system.

When it detects a virus or other malware, the Bitdefender agent will automatically attempt to remove the malware code from the infected file and reconstruct the original file. This operation is referred to as disinfection. Files that cannot be disinfected are moved to quarantine in order to isolate the infection. When a file containing malware is in quarantine, it cannot do any harm because it cannot be executed or read. If you do not want specific files or file types to be scanned, you can configure scan exclusions.

The settings are organized into the following tabs:

- On Access
- On Demand
- Exclusions
- Quarantine

On Access

Option	Description
On Access Scanning	On-access scanning prevents new malware threats from entering the system by scanning local and network files when they are accessed (opened, moved, copied or executed), boot sectors and potentially unwanted applications (PUA). **DEFAULT:** Enabled, Scan mode: Normal, Action: Disinfect
Advanced Threat Control	Bitdefender Advanced Threat Control (ATC) is an innovative proactive detection technology, which uses advanced heuristic methods to detect new potential threats in real time. ATC continuously monitors the applications running on the computer, looking for malware-like actions. Each of these actions is scored and an overall score is computed for each process. When the overall score for a process reaches a given threshold, the process is considered to be harmful. Active Threat Control will automatically try to disinfect the detected file. **DEFAULT:** Enabled, Scan mode: Normal, Action: Disinfect

On Demand

Option	Description
Scan Tasks	You can add and configure the following types of scan tasks: • **Quick Scan**, which uses in-the-cloud scanning to detect malware running in the system. Running a Quick Scan usually takes less than a minute and uses a fraction of the system resources needed by a regular malware scan. You can add only one quick scan task for the same policy. • **Full Scan**, which checks the entire computer for all types of malware. You can add only one full scan task for the same policy. • **Custom Scan**, which allows you to choose the specific locations to be scanned and to configure the scan options. • **Network Scan**, which is a type of custom scan that allows assigning one single managed computer to scan network drives, then configuring the scan options and the specific locations to be scanned. For network scan tasks, you must enter the credentials of a user account with read/write permissions on the target network drives, so that the security agent will be able to access and take actions on these network drives. **DEFAULT:** Blank
Device Scanning	You can configure the agent to automatically detect and scan external storage devices connected to the computer, and disinfect files or move them to quarantine if disinfection is not possible. Detected devices fall into one of these categories: • CDs/DVDs • Mapped network drives • Devices with more than a specified amount of stored data.

Option	Description
	DEFAULT: Enabled
CD/DVD Media	See **Device Scanning**. **DEFAULT:** Enabled
Mapped network drives	See **Device Scanning**. **DEFAULT:** Disabled
Do not scan devices with stored data more than (MB)	See **Device Scanning**. Use this option to automatically skip scanning of a detected device if the amount of stored data exceeds the specified size. Type the size limit (in megabytes) in the corresponding field. Zero means that no size restriction is imposed. **DEFAULT:** Disabled

Exclusions

Option	Description
Active Exclusions	When enabled, the agent excludes from scanning certain objects with infinitesimal probability of infection and objects in the Exclusion list, if defined. **DEFAULT:** Enabled
Exclusions list	When scanning exclusions are active, you can also add custom exclusions, according to your specific needs. Custom exclusions can apply to on-access scanning or on-demand scanning, or to both. Based on the object of the exclusion, there are four types of exclusions: • File exclusions: the specified file only is excluded from scanning. • Folder exclusions: all files inside the specified folder and all of its subfolders are excluded from scanning. • Extension exclusions: all files having the specified extension are excluded from scanning. • Process exclusions: any object accessed by the excluded process is also excluded from scanning.

Option	Description
	DEFAULT: Blank

Quarantine

Option	Description
Delete files older than (days)	Choose the lifetime of the quarantined files, expressed in days. After this interval, the files will be automatically deleted. **DEFAULT:** 30
Submit quarantined files to Bitdefender Labs every (hours)	Select the time interval when quarantined files are being sent to Bitdefender Labs to be analyzed. If malware presence is confirmed, a signature is released to allow removing the malware. **DEFAULT:** Enabled, 1
Rescan quarantine after malware signatures update	Keep this option selected to automatically scan quarantined files after each malware signatures update. Cleaned files are automatically moved back to their original location. **DEFAULT:** Enabled
Copy files to quarantine before applying the disinfect action	Select this option to prevent data loss in case of false positives and copy each infected file to quarantine before disinfection. **DEFAULT:** Enabled

8. QUARANTINE

The quarantine is an encrypted folder on the endpoint, which contains potentially malicious files, such as malware-suspected, malware-infected or other unwanted files. When a virus or other form of malware is in quarantine, it cannot do any harm because it cannot be executed or read.

Bitdefender moves files to quarantine according to the policies assigned to endpoints. By default, files that cannot be disinfected are quarantined.

Quarantined files are automatically sent to Bitdefender Labs in order to be analyzed by the Bitdefender malware researchers. If malware presence is confirmed, a signature is released to allow removing the malware. In addition, quarantined files are scanned after each malware signature update. Cleaned files are automatically moved back to their original location.

To change the default agent behavior and quarantine settings, refer to " Quarantine " (p. 27)

8.1. Exploring the Quarantine

The quarantine has three different levels of visibility in LabTech Control Center:

- **General**, showing files from all protected computers of all Clients.
- **Client**, showing files from all protected computers of the selected Client.
- **Computer**, showing files only from the selected computer.

To view the entire quarantine:

1. Click the **Bitdefender** button on the LabTech Toolbar to open the Plugin Dashboard.
2. Select the **Quarantine** tab.

To view the quarantine for a specific client:

1. Expand the **Clients** group in the **Navigation Tree**.
2. Double-click the selected client to open the Client Screen.
3. Select the **Bitdefender > Quarantine** tab.

To view the quarantine from a specific computer:

1. Expand the **Clients > location** group in the **Navigation Tree**.

2. Double-click the computer you are interested in to open the Computer Screen.
3. Select the **Bitdefender > Quarantine** tab.

The Quarantine table displays information about quarantined files such as file location, detected malware, last signatures update that the file was checked against, and the action status.

You can also make the information available out of the LabTech Control Center in case you want to process the information. Click the **Export to Excel** button at the upper-right corner of the tab to save the data in a Microsoft Excel file.

8.2. Restoring Quarantined Files

On particular occasions, you may need to restore quarantined files, either to their original location or to an alternate location. One such situation is when you want to recover important files stored in an infected archive that has been quarantined.

To a restore a quarantined file:

1. Select the file in the Quarantine table.
2. Click the **Restore file** button at the upper right corner of the tab.
3. Choose the location where you want the selected file to be restored (either the original or a custom location on the target computer).

   If you choose to restore to a custom location, you must enter the absolute path in the corresponding field.
4. Select **Automatically add exclusion** in policy to exclude the file to be restored from future scans. The exclusion applies unless the default policy, which cannot be modified, is assigned.
5. Click **Save**. You can notice the pending status in the **Action** column. Once a file is restored, the corresponding entry will disappear from the Quarantine table.

8.3. Deleting Quarantined Files

By default, quarantined files older than 30 days are automatically deleted. This setting can be changed by editing the policy assigned to the managed computers.

If you want to manually delete quarantined files, you should first make sure the files you choose to delete are not needed.

A file may actually be the malware itself. If your research leads you to such a situation, you can search the quarantine for the specific threat and delete it from the quarantine.

To delete one or more quarantined files:

1. In the Quarantine table, select the quarantined files you want to delete.
2. Click the **Remove file** button at the upper right corner of the tab. You will have to confirm your action by clicking **Yes**.

   You can notice the pending status in the **Action** column. Once a file is deleted, the corresponding entry will disappear from the Quarantine table.

9. REPORTS

Bitdefender Plugin comes with four predefined report types, informing you on the security status of the remote computers protected by the Bitdefender agent. The reports help you identify threats and vulnerabilities, monitor security incidents and malware activity, and assess the network security.

9.1. Using Reports

Depending on the target, reports are available at three different levels.

Global Level Reports

The reports centralize data from all protected computers of all clients.

To view global reports:

1. Click the **Bitdefender** button on the LabTech Toolbar to open the Plugin Dashboard.
2. Select the **Main** tab.

Client Level Reports

The reports collect data from all protected computers of the selected client.

To view reports related to a specific client:

1. Expand the **Clients** group in the **Navigation Tree**.
2. Double-click the selected client to open the Client Screen.
3. Select the **Bitdefender > Main** tab.

Computer Level Reports

The reports collect data only from the selected computer.

To view reports related to a specific computer:

1. Expand the **Clients > location** group in the **Navigation Tree**.
2. Double-click the computer you are interested in to open the Computer Screen.
3. Select the **Bitdefender > Main** tab.

The **Main** tab consists of a summary section (the upper half of the tab) and a details section (the lower half of the tab).

The summary section displays graphical charts from all available reports, allowing you to quickly evaluate the security status of the remote computers.

Click each chart to view the related data in the details section.

Note
Reports refer to the data collected only from the last seven days.

To make sure the latest information is being displayed, click the **Update** button at the right side of the tab, below the charts.

The reports in LabTech Control Center only allow you to sort and filter the information. To sort reports by a specific column, simply click the header of that column. Click the column header again to change the sorting order. To easily find what you are looking for, use the Filter icon at the right side of the column and then select the proper option from the drop-down list.

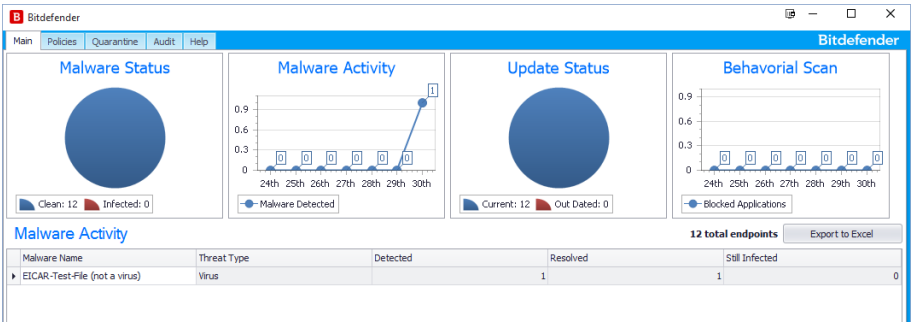
If you want a more complex analysis and process the data, you can simply save the details of the report to an XLS file by clicking the **Export to Excel** button at the lower-left corner of the tab.

9.2. Report Types

Malware Activity

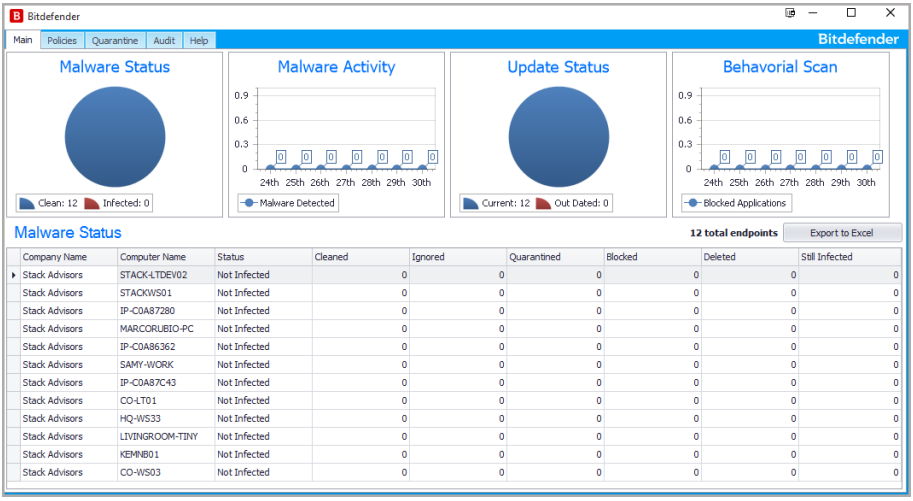
This report displays information on detected malware, but does not relate it to any specific computer. You can view:

- Number of files detected with malware.
- Number of resolved infections. These files have been successfully disinfected or moved to quarantine.
- Number of files still infected. These files could not be disinfected, because access is denied. For example, an infected file stored in some proprietary archive format or protected by password.



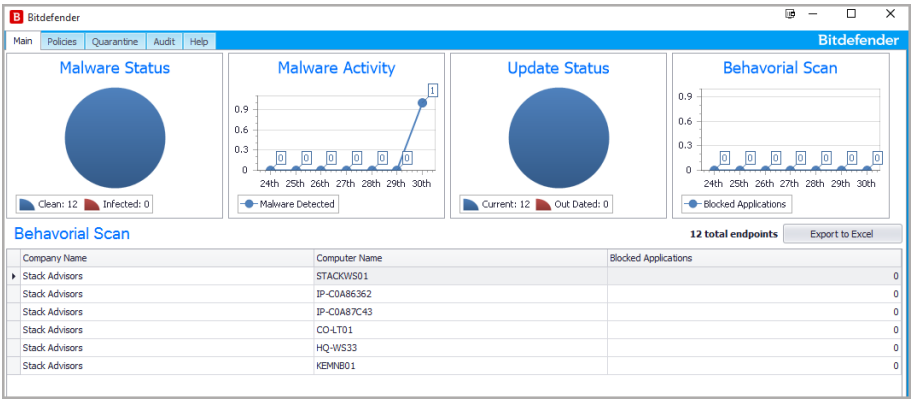
Malware Status

The report helps you find out how many and which of the selected computers have been affected by malware. For each computer, you can view its current protection status, as well as the number of files detected with malware, broken down by the actions taken.



Behavioral Scan

This report displays the number of blocked applications for the selected computers.

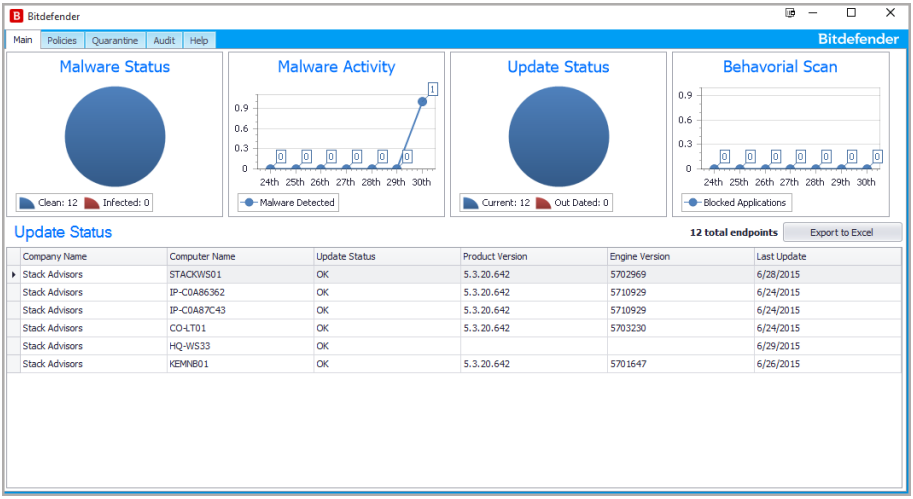


Company Name	Computer Name	Blocked Applications
Stack Advisors	STACKWS01	0
Stack Advisors	IP-C0A86362	0
Stack Advisors	IP-C0A87C43	0
Stack Advisors	CO-LT01	0
Stack Advisors	HQ-WS33	0
Stack Advisors	KEMNB01	0

Update Status

This report shows you the update status of the Bitdefender agent installed on selected computers. The update status refers to product version and engines (signatures) version.

Using the available filters, you can easily find out which clients have updated and which have not in the last 24 hours.



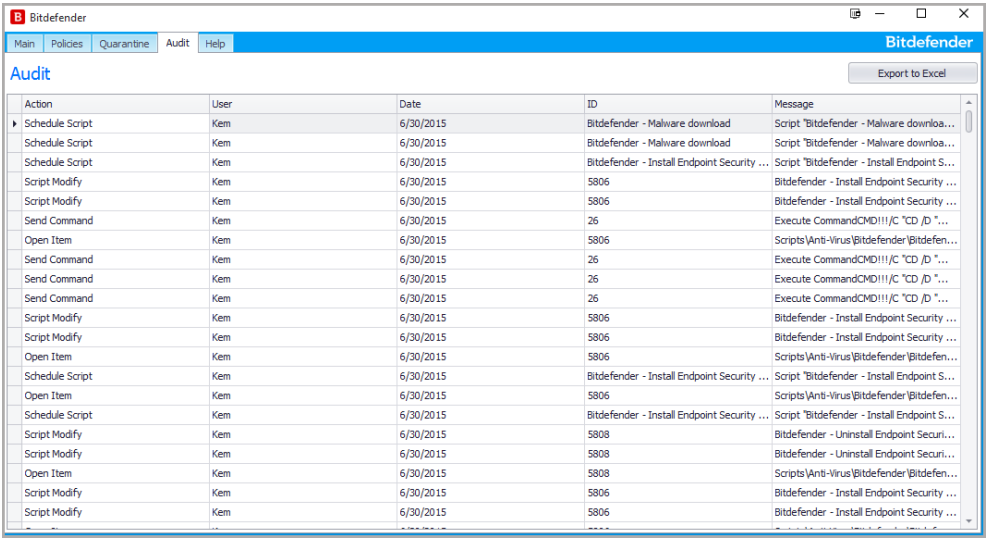
Company Name	Computer Name	Update Status	Product Version	Engine Version	Last Update
Stack Advisors	STACKWS01	OK	5.3.20.642	5702969	6/28/2015
Stack Advisors	IP-C0A86362	OK	5.3.20.642	5710929	6/24/2015
Stack Advisors	IP-C0A87C43	OK	5.3.20.642	5710929	6/24/2015
Stack Advisors	CO-LT01	OK	5.3.20.642	5703230	6/24/2015
Stack Advisors	HQ-WS33	OK			6/29/2015
Stack Advisors	KEMNB01	OK	5.3.20.642	5701647	6/26/2015

10. AUDIT LOGS

The plugin logs actions performed by users related to Bitdefender installation and policies.

To examine the log records:

1. Click the **Bitdefender** button from the LabTech Toolbar to open the Plugin Dashboard.
2. Select the **Audit** tab. Events are organized in a table, each line representing an event record.



Action	User	Date	ID	Message
Schedule Script	Kem	6/30/2015	Bitdefender - Malware download	Script "Bitdefender - Malware downloa...
Schedule Script	Kem	6/30/2015	Bitdefender - Malware download	Script "Bitdefender - Malware downloa...
Schedule Script	Kem	6/30/2015	Bitdefender - Install Endpoint Security ...	Script "Bitdefender - Install Endpoint S...
Script Modify	Kem	6/30/2015	5806	Bitdefender - Install Endpoint Security ...
Script Modify	Kem	6/30/2015	5806	Bitdefender - Install Endpoint Security ...
Send Command	Kem	6/30/2015	26	Execute CommandCMD!!!/C "CD /D "...
Open Item	Kem	6/30/2015	5806	Scripts\Anti-Virus\Bitdefender\Bitdefen...
Send Command	Kem	6/30/2015	26	Execute CommandCMD!!!/C "CD /D "...
Send Command	Kem	6/30/2015	26	Execute CommandCMD!!!/C "CD /D "...
Send Command	Kem	6/30/2015	26	Execute CommandCMD!!!/C "CD /D "...
Script Modify	Kem	6/30/2015	5806	Bitdefender - Install Endpoint Security ...
Script Modify	Kem	6/30/2015	5806	Bitdefender - Install Endpoint Security ...
Open Item	Kem	6/30/2015	5806	Scripts\Anti-Virus\Bitdefender\Bitdefen...
Schedule Script	Kem	6/30/2015	Bitdefender - Install Endpoint Security ...	Script "Bitdefender - Install Endpoint S...
Open Item	Kem	6/30/2015	5806	Scripts\Anti-Virus\Bitdefender\Bitdefen...
Schedule Script	Kem	6/30/2015	Bitdefender - Install Endpoint Security ...	Script "Bitdefender - Install Endpoint S...
Script Modify	Kem	6/30/2015	5808	Bitdefender - Uninstall Endpoint Securi...
Script Modify	Kem	6/30/2015	5808	Bitdefender - Uninstall Endpoint Securi...
Open Item	Kem	6/30/2015	5808	Scripts\Anti-Virus\Bitdefender\Bitdefen...
Script Modify	Kem	6/30/2015	5806	Bitdefender - Install Endpoint Security ...
Script Modify	Kem	6/30/2015	5806	Bitdefender - Install Endpoint Security ...

Each record contains information such as:

- Type of the action that caused the event.
- The user who performed the action.
- Time and date of the event.
- Name of the affected client, computer and policy (if applicable).

To sort events by a specific column, simply click the header of that column. Click the column header again to reverse the sorting order.

To filter events:

1. Move the mouse cursor over the column header.
2. Click the Filter icon at the right side of the column and then select an option from the drop-down list.

   To define a complex filter criteria, select the option **(Custom)**.

11. UNINSTALLATION

11.1. Uninstalling the Agent

To uninstall the security agent from endpoints in LabTech system:

1. Expand the **Clients** group in the **Navigation Tree**.
2. Open the Client screen of the organization where the endpoints are located.
3. Select the **Bitdefender > Deploy** tab.
4. From the **Filter** menu at the upper left corner of the tab, select **Installed**.
5. Select the computers from which you want to uninstall the agent.
6. Click the **Uninstall** button at the upper right side of the tab. A pop-up window will confirm the operation. If the uninstallation fails, a ticket will be generated.

Note
You can also uninstall the agent from a specific computer using the **Bitdefender > Deploy** tab of the Computer screen.

11.2. Uninstalling the Plugin

To uninstall the Bitdefender Plugin from your LabTech system:

1. From the **Main Menu** bar, select **Help > Plugin Manager**.
2. From the **Advanced** drop-down, select **Manage Plugins > Remove Plugin**.
3. Click **Yes** when prompted to confirm the removal.

   This operation will remove the plugin files only, leaving the database with the configuration settings intact if you want to reinstall the plugin.

Note
For more information, refer to Using the Plugin Manager section of the LabTech documentation.

To completely remove the Plugin, including the configurations made:

1. Uninstall the plugin from **LabTech Plugin Manager**, as previously described.
2.
3. Extract the script from the archive.

4. Import the script in SQL server.
5. Run the script.

12. GETTING HELP

Bitdefender strives to provide its customers with an unparalleled level of fast and accurate support.

If you experience any issue with or if you have any question about your Bitdefender product, go to our online Support Center. It provides several resources that you can use to quickly find a solution or an answer.

Or, if you prefer, you can contact the Bitdefender Customer Care team. Our support representatives will answer your questions in a timely manner and they will provide you with the assistance you need.

12.1. Bitdefender Support Center

Bitdefender Support Center is the place where you will find all the assistance you need with your Bitdefender product.

You can use several resources to quickly find a solution or an answer:

- Knowledge Base Articles
- Bitdefender Support Forum
- Product Documentation

You can also use your favorite search engine to find out more information about computer security, the Bitdefender products and the company.

Knowledge Base Articles

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

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

The Bitdefender Knowledge Base for business products is available any time at http://www.bitdefender.com/support/business.html.

Bitdefender Support Forum

The Bitdefender Support Forum provides Bitdefender users with an easy way to get help and to help others. You can post any problem or question related to your Bitdefender product.

Bitdefender support technicians monitor the forum for new posts in order to assist you. You may also get an answer or a solution from a more experienced Bitdefender user.

Before posting your problem or question, please search the forum for a similar or related topic.

The Bitdefender Support Forum is available at http://forum.bitdefender.com, in 5 different languages: English, German, French, Spanish and Romanian. Click the **Business Protection** link to access the section dedicated to business products.

Product Documentation

Product documentation is the most complete source of information about your product.

You can check and download the latest version of the documentation either the from Bitdefender Plugin interface or from the **Documentation** section available on product support page.

12.2. Asking for Assistance

You can contact us for assistance through our online Support Center:

1. Go to http://www.bitdefender.com/support/contact-us.html.
2. Use the contact form to open an email support ticket or access other available contact options.

12.3. Contact Information

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

Web Addresses

Sales Department: enterprisesales@bitdefender.com
Technical Support: businesspartners@bitdefender.com
Documentation: documentation@bitdefender.com
Local Distributors: http://www.bitdefender.com/partners
Virus Submissions: virus_submission@bitdefender.com
Report Abuse: abuse@bitdefender.com
Website: http://www.bitdefender.com/business/service-providers.html
Website: http://www.bitdefender.com

Local Distributors

The Bitdefender local distributors are ready to respond to any inquiries regarding their areas of operation, both in commercial and in general matters.

To find a Bitdefender distributor in your country:

1. Go to http://www.bitdefender.com/partners.
2. Go to **Partner Locator**.
3. The contact information of the Bitdefender local distributors should be displayed automatically. If this does not happen, select the country you reside in to view the information.
4. If you do not find a Bitdefender distributor in your country, feel free to contact us by email at businesspartners@bitdefender.com.

Bitdefender Office

The Bitdefender office is ready to respond to any inquiries regarding its areas of operation, both in commercial and in general matters.

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
United States
Phone: (+1) 954 414 9631
Email: businesspartners@bitdefender.com
Web: http://www.bitdefender.com
Support Center: http://www.bitdefender.com/support/business.html