

*End-User Guide*

# **GFI** OneGuard™

*Information for end-users on how to use the features available in the GFI OneGuard agent on managed devices.*



The information and content in this document is provided for informational purposes only and is provided "as is" with no warranties of any kind, either express or implied, including without limitation any warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software disclaims and in no event shall be liable for any losses or damages of any kind, including any consequential or incidental damages in connection with the furnishing, performance or use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no warranty, promise or guarantee about the completeness, accuracy, recency or adequacy of information contained in this document and is not responsible for misprints, out-of-date information, or errors. GFI reserves the right to revise or update its products, software or documentation without notice. You must take full responsibility for your use and application of any GFI product or service. No part of this documentation may be reproduced in any form by any means without prior written authorization of GFI Software.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

GFI and GFI OneGuard are trademarks or registered trademarks of GFI Software or its affiliates in the US and other countries. Any other trademarks contained herein are the property of their respective owners.

GFI OneGuard is copyright of GFI Software. - 1999-2017 GFI Software. All rights reserved.

Document Version: 1.0

Last updated (month/day/year): 06/21/2017

# Contents

<b>1 Introduction</b> .....	<b>4</b>
<b>2 Using the Antivirus Agent</b> .....	<b>5</b>
2.1 Antivirus scans .....	6
2.2 Quarantine .....	7
2.3 Backup of malicious files .....	9
2.4 Unprocessed files .....	10
2.5 Reports .....	10
2.6 Antivirus Agent settings .....	12

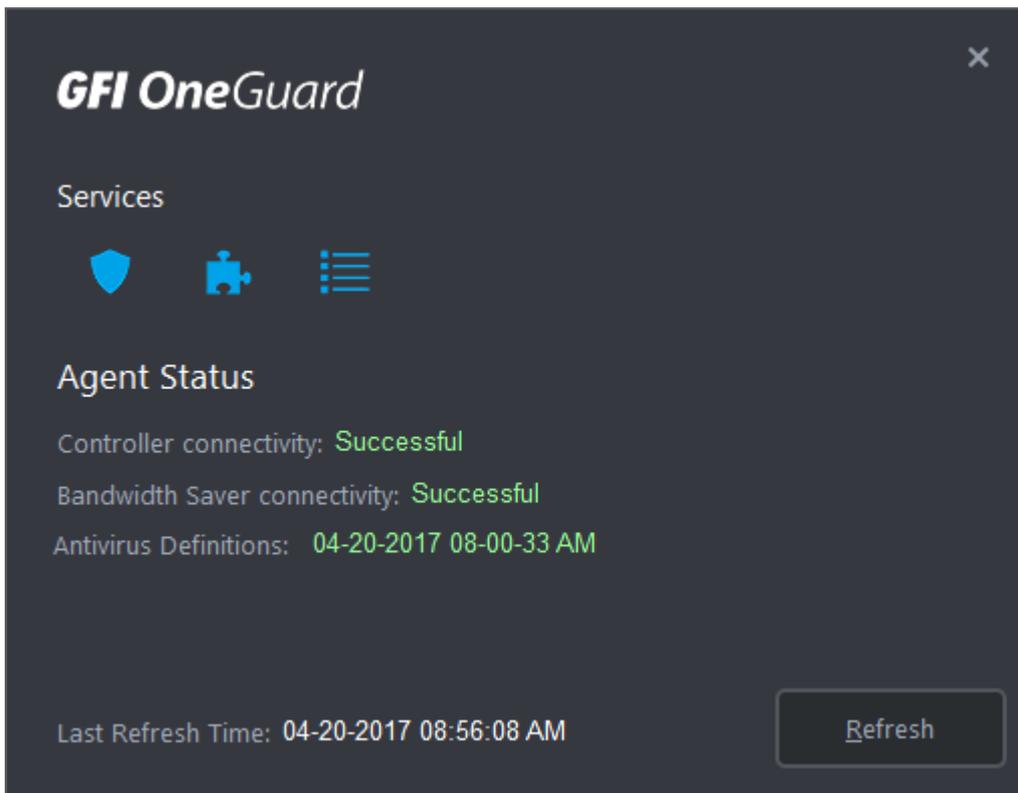
## 1 Introduction

The GFI OneGuard agent is a software that enables your organization to remotely manage various services on your computer, such as antivirus and patch management.

This help system provides information to end-users on how to use the features available by the GFI OneGuard agent, including the antivirus agent which protects your computer from viruses and malware threats.

When deployed on a network machine, the GFI OneGuard Agent can be accessed from the system tray of that machine.

Right-click the GFI OneGuard icon  and select **Status**. The GFI OneGuard Agent Status window shows the connectivity of the Agent with the GFI OneGuard Controller and connectivity with the Bandwidth Saver server. Contact your administrator if you encounter any connectivity issues.



Screenshot 1: Monitoring the status of the GFI OneGuard Agent

## 2 Using the Antivirus Agent

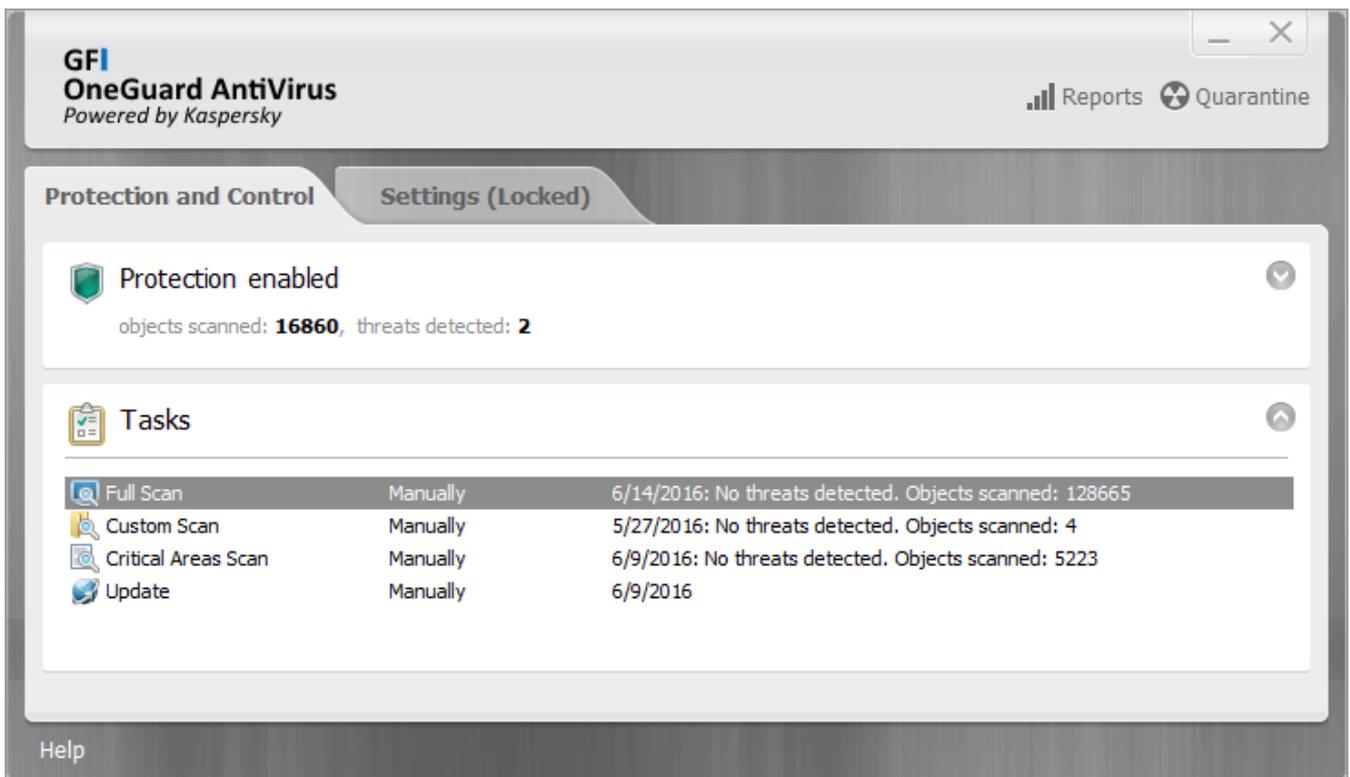
Users can perform antivirus scans from their machine using the GFI OneGuard Antivirus agent. The antivirus engine in GFI OneGuard is powered by Kaspersky Lab.



This agent also provides task scheduling and reporting features, as well as a quarantine area where infected files are safely stored. The Antivirus agent is accessible from the system tray of managed devices. To open the main window of the Antivirus Agent, right click on the system tray and select the **GFI OneGuard Antivirus** icon .

### NOTE

Certain actions, like changing settings or deleting files from quarantine, can only be performed by network administrators.



Screenshot 2: GFI OneGuard Antivirus Agent User Interface

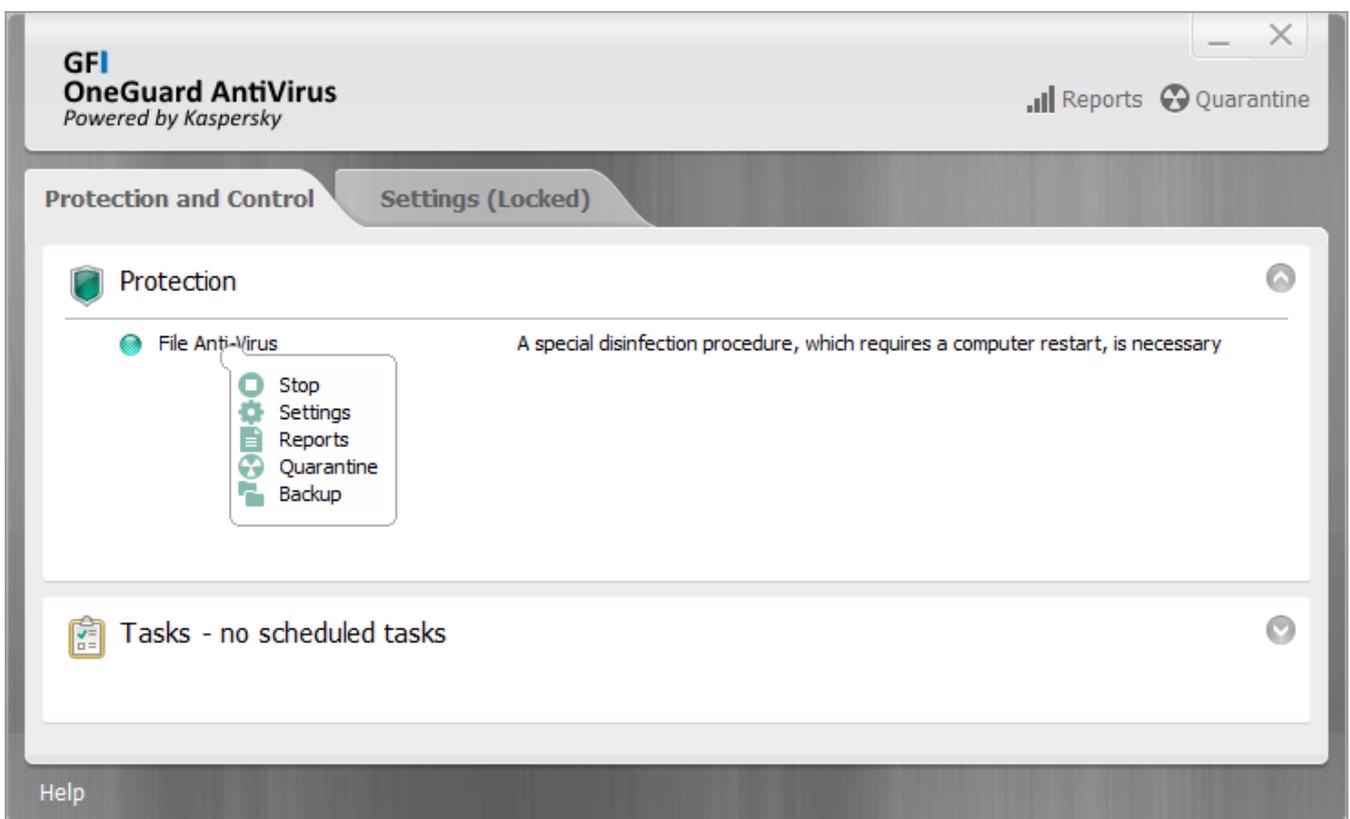
The main window of the Antivirus Agent contains the following elements:

Option	Description
<b>Protection and Control</b>	Review the scan status and trigger manual antivirus scans on your machine.
<b>Settings</b>	View antivirus settings. Settings are not editable since these are centrally managed by your network administrator.

Option	Description
<b>Reports</b>	View reports about the operation of the Antivirus Agent in general and the operation of individual application components, scan tasks, update tasks, and vulnerability scan tasks.
<b>Quarantine</b>	Review items that the antivirus agent detected as infected.
<b>Unprocessed files</b>	Information about files that the antivirus agent could not scan or process.
<b>Backup</b>	Access copies of files that were deleted or disinfected by the antivirus agent.
<b>Help</b>	Opens the help system of the GFI OneGuard Antivirus Agent.

## 2.1 Antivirus scans

From the GFI OneGuard Antivirus Agent, end users can trigger new scans and monitor scan results.



Screenshot 3: GFI OneGuard Antivirus User Interface

From the GFI OneGuard Antivirus Agent interface, click the **Protection and Control** tab to manage antivirus scans. Scan components and tasks are grouped into two sections, based on the actions that the Antivirus Agent takes to protect the operating system against different threats. Click the  or  icons to expand or hide the following sections:

Section	Description
<b>Protection</b>	Shows the status of real time file protection (Active Protection) and any detected threats.

Section	Description
<b>Tasks</b>	<p>A list of scans and tasks that can be triggered and their status. Click a task and choose the action to perform:</p> <ul style="list-style-type: none"> <li>» <b>Start scanning</b> - Starts an antivirus scan on the files that fall within the scope of the chosen scan type.</li> <li>» <b>Scan scope</b> - Select folders and files to be scanned by Antivirus Agent while performing the selected task.</li> <li>» <b>Start update</b> - Initiates an antivirus database and application module update task.</li> <li>» <b>Roll back update</b> - Reverts the application to the previous version of the update package.</li> <li>» <b>Settings</b> - Opens the settings of the selected component or task. Settings are not editable. For more information, refer to <a href="#">Antivirus Agent settings</a> (page 12).</li> <li>» <b>Reports</b> - Opens a report on the events that occurred while a component or task was active. For more information, refer to <a href="#">Reports</a> (page 10).</li> <li>» <b>Quarantine</b> - Opens the Quarantine area. For more information, refer to <a href="#">Quarantine</a> (page 7).</li> <li>» <b>Backup</b> - Opens the Backup area. For more information, refer to <a href="#">Backup of malicious files</a> (page 9).</li> </ul> <p>The following information is displayed for each task:</p> <ul style="list-style-type: none"> <li>» Task name</li> <li>» Task status</li> <li>» Statistics and progress status of a task that is running or has been stopped. The statistics are shown on the right of the task status.</li> <li>» Statistics of the last instance of a task that has been completed. The statistics are shown on the right of the task status.</li> <li>» Error description, if the task completes with an error. The description is shown on the right of the task status.</li> </ul>

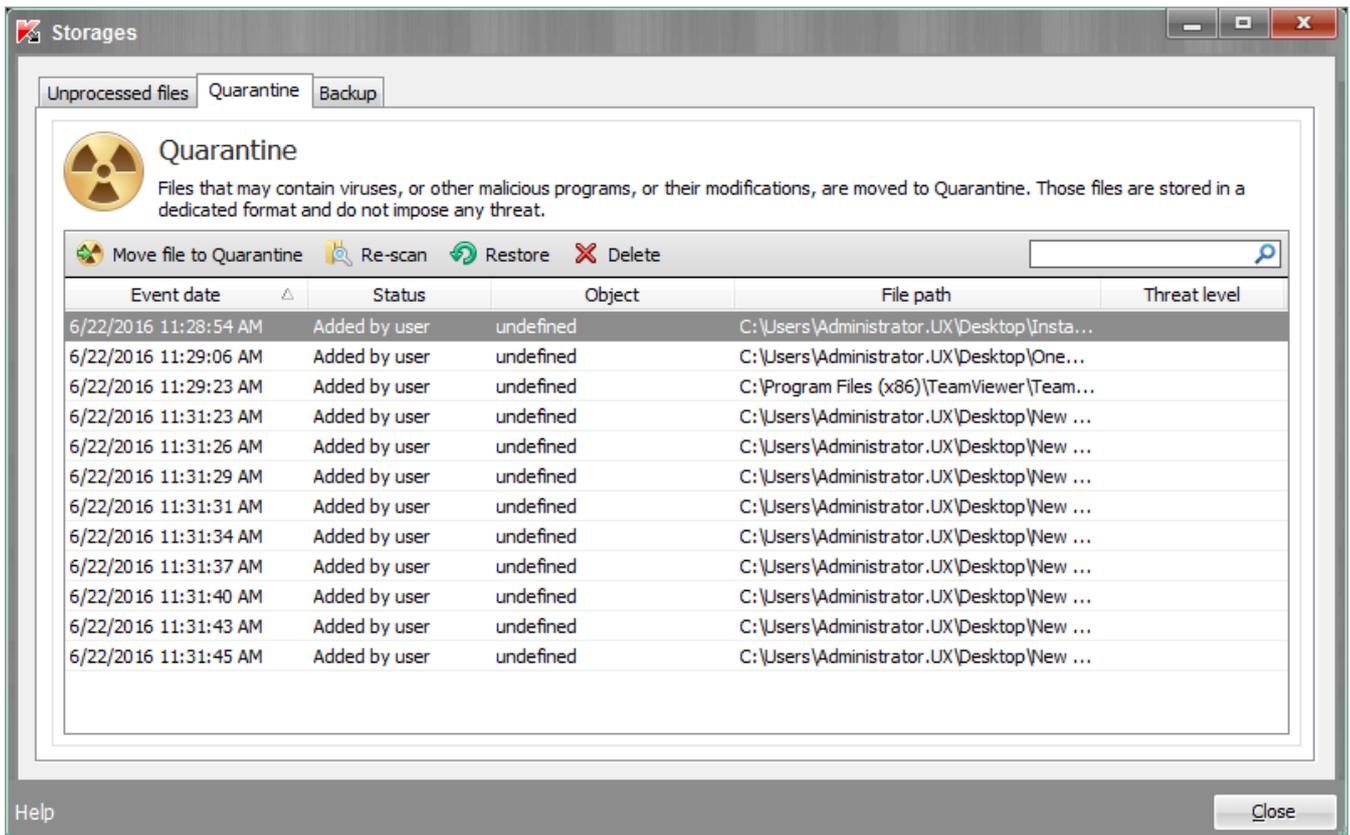
## 2.2 Quarantine

The Quarantine is a list of files which the antivirus agent detects as infected. These files may contain viruses and other threats or their varieties.

When GFI OneGuard Antivirus agent quarantines a file, it does not copy the file, but moves it. The application deletes the file from the hard drive or email message and saves the file in a special data storage. Files in Quarantine are encrypted and do not pose a threat.

GFI OneGuard Antivirus agent detects and quarantines a probably infected file during a virus scan. You can also manually move a file that you suspect of containing viruses or other malware in Quarantine.

By default, the Antivirus agent permanently deletes files from Quarantine after a number of days, as configured by your network administrator (default is 30 days).



Screenshot 4: GFI OneGuard Antivirus Quarantine area

GFI OneGuard Antivirus agent places files in Quarantine in the following cases:

- » File code resembles a known but partly modified malicious program, or has a malware-like structure, and is not listed in the Antivirus agent's database. In this case, the file is placed in Quarantine after heuristic analysis by File Anti-Virus and Mail Anti-Virus, or during a virus scan. Heuristic analysis rarely causes false positives.
- » The sequence of operations that a file performs is dangerous. In this case, the file is placed in Quarantine after the System Watcher component has analyzed its behavior.

The following file operations are available when managing Quarantine:

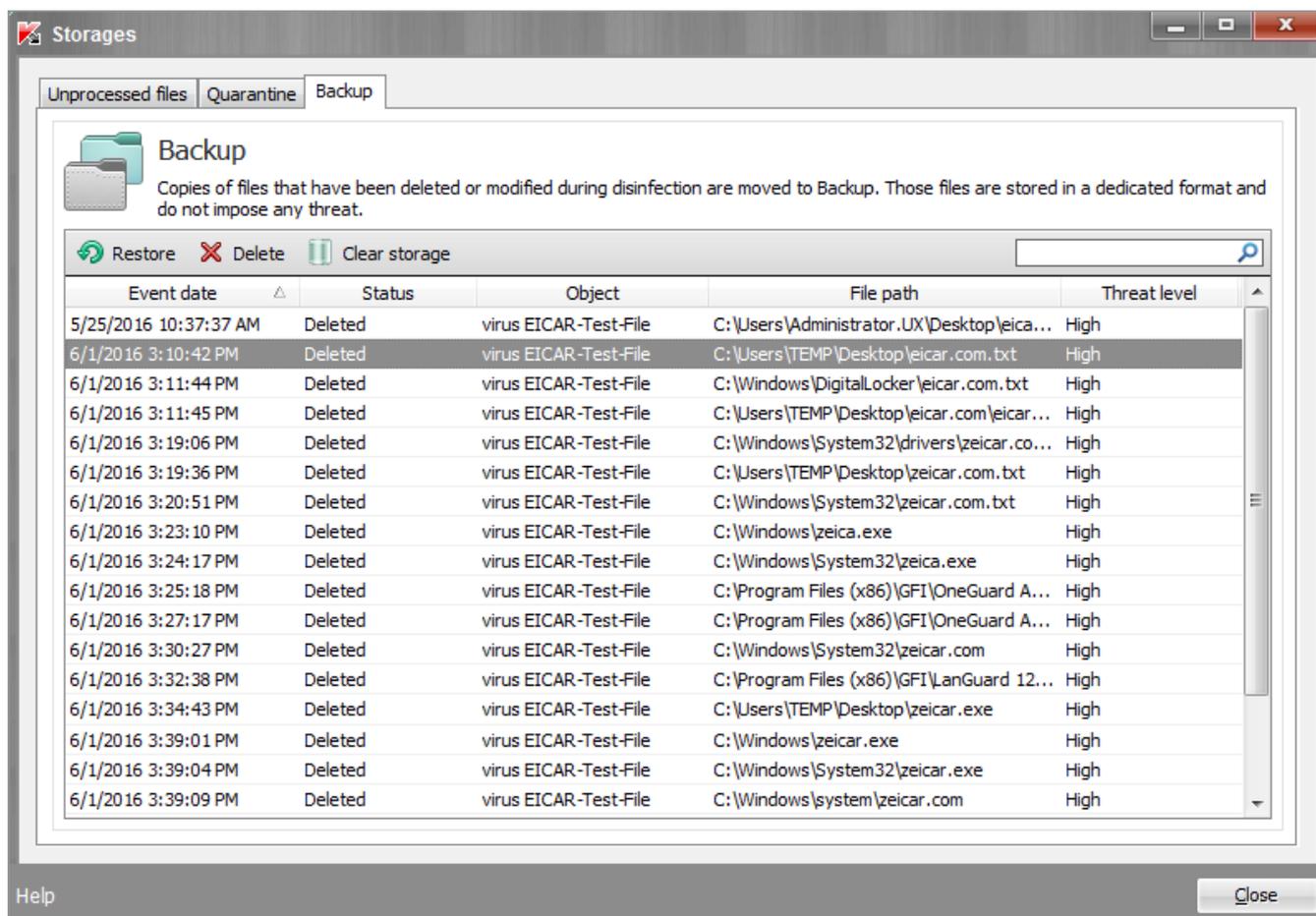
Action	Description
View quarantined files	The list of quarantined files is shown in the <b>Quarantine</b> tab.
Manually moving a file to Quarantine	You can manually quarantine a file that you suspect of containing viruses or other threats. To do this, click <b>Move file to Quarantine</b> and select the file to quarantine. Click <b>Open</b> . The file is now moved from its original folder to Quarantine and access to this file from disk is blocked.
Re-scan quarantined files	Right-click a quarantined file and click <b>Re-scan</b> to scan it using the current version of the Antivirus agent databases and modules. A notification shows the re-scan results and the number of detected threats.
Restore files to their original folders	To restore ALL quarantined files to their original folders, right-click anywhere in the table on the Quarantine tab to display the context menu and select <b>Restore all</b> . To restore one or more quarantined files, select one or more files to restore and click <b>Restore</b> . The Antivirus agent restores the selected files to their original folders.
Deleting quarantined files	To manually delete one or more files from quarantine permanently, select one or more files to delete and click <b>Delete</b> .

## 2.3 Backup of malicious files

If malicious code is detected in a file, the GFI OneGuard Antivirus agent blocks the file, removes it from its original folder, places its copy in Backup, and attempts to disinfect it. If file disinfection succeeds, the status of the backup copy of the file changes to Disinfected. You can restore the file from its disinfected backup copy to its original folder.

GFI OneGuard Antivirus agent automatically deletes backup copies of files with any status from Backup after a set period (by default 30 days, but configurable by administrator). You can also manually delete the backup copy.

To view a list of files in Backup, open the Antivirus agent main application window. In the upper part of the main application window, click **Quarantine**, then select the **Backup** tab.



Screenshot 5: GFI OneGuard Antivirus Backup area

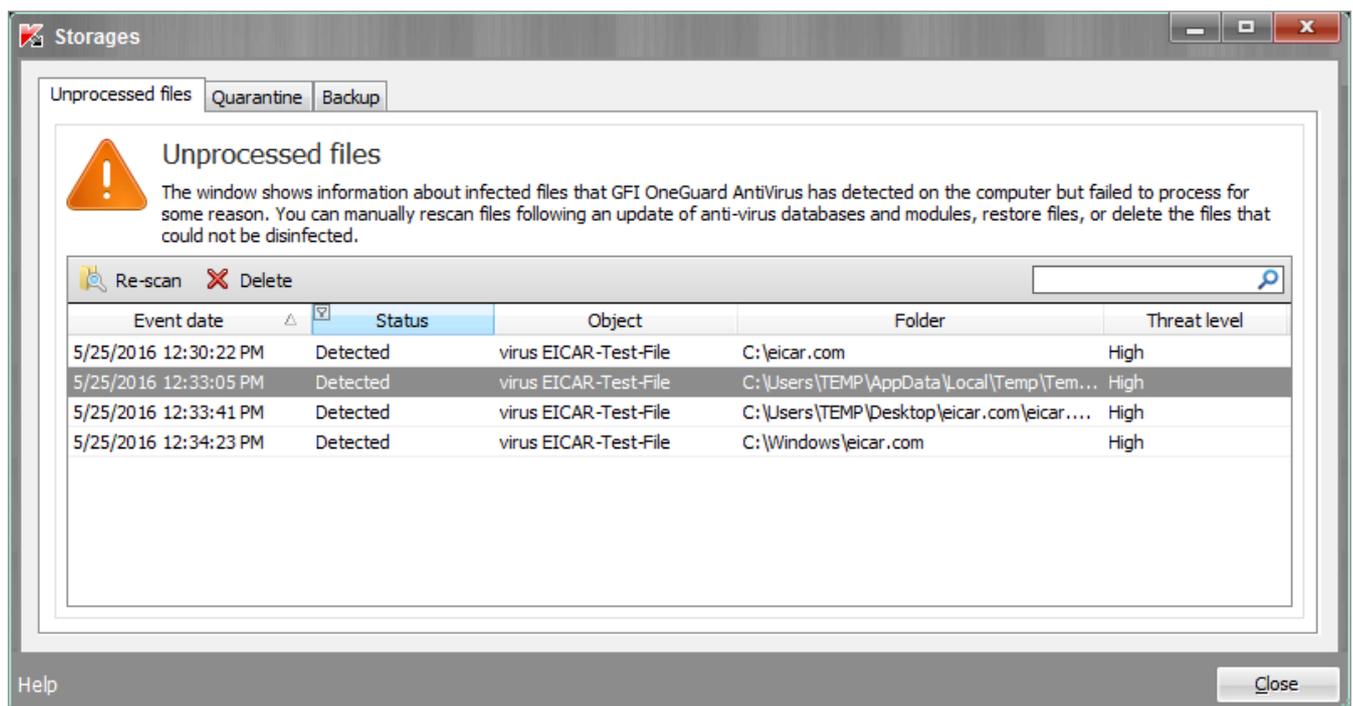
While managing Backup, you can perform the following actions with backup copies of files:

Action	Description
Restore files from backup copies to their original folders	Select one or more Backup events and click <b>Restore</b> . It is highly recommended to restore files only when they have a <b>Disinfected</b> status. Note that sometimes it is not possible to maintain the integrity of files during disinfection. If you partially or completely lose access to important information in a disinfected file after disinfection, you can attempt to restore the disinfected copy of the file to its original folder.
Delete backup file copies	To permanently delete backup copies of files from Backup, select one or more Backup events and click <b>Remove</b> .
Delete all backup copies	Click <b>Clear Storage</b> to permanently delete all the files from the Backup list.

## 2.4 Unprocessed files

GFI OneGuard Antivirus agent logs information about infected files that it could not process for some reason. If GFI OneGuard Antivirus agent fails to disinfect or remove an infected file, then that file is considered unprocessed. This situation is typically encountered when the infected file is unavailable (for example, file located on a removable drive without write privileges).

To view a list of unprocessed files, open the Antivirus agent main application window. In the upper part of the main application window, click **Quarantine**, then select the **Unprocessed files** tab.



Screenshot 6: GFI OneGuard Antivirus unprocessed files area

You can perform the following file operations while managing the list of unprocessed files:

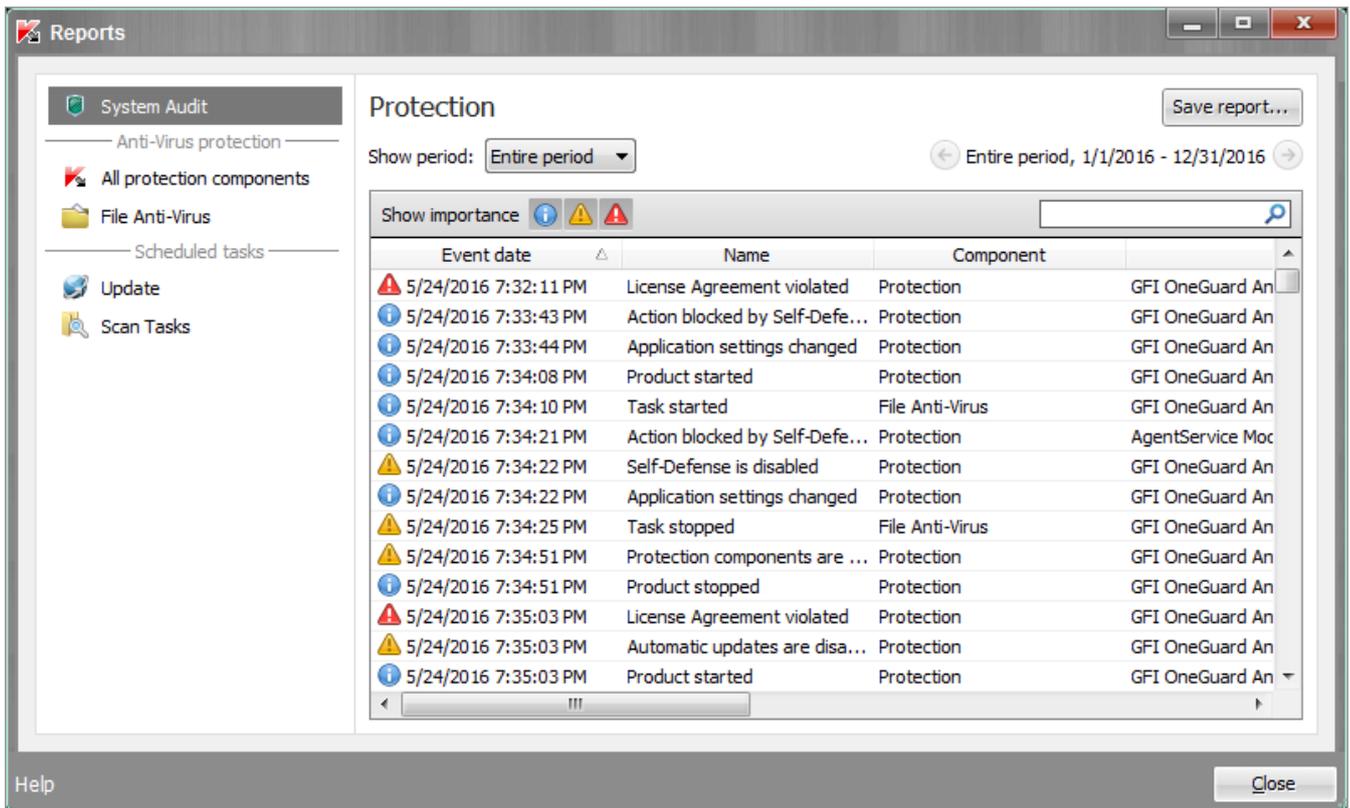
Action	Description
Re-scan the files	Scan unprocessed files using the current version of GFI OneGuard Antivirus agent databases and modules. Select one or more Unprocessed files and click <b>Re-scan</b> .
Delete unprocessed files	To delete unprocessed files, select one or more unprocessed files and click <b>Remove</b> .

## 2.5 Reports

The reports area provides information about the operation of the GFI OneGuard Antivirus component, performance of each scan task, update task, and vulnerability scan task.

To view reports:

1. Open the main application window.
2. In the upper part of the main application window, click **Reports**.



Screenshot 7: GFI OneGuard Antivirus reports

3. To generate a report, use the following options:

Option	Description
<b>System Audit</b>	Contains information about events occurring during the interaction between the user and the application and in the course of application operation in general.
<b>All Protection Components</b>	Information about events that are logged in the course of operation of the GFI OneGuard Antivirus Agent.
<b>File Antivirus</b>	Contains information about events that occur during the operation of the File Antivirus component.
<b>Update</b>	Click to view only update tasks.
<b>Scan Tasks</b>	Click to view a list of scan tasks.
<b>Show period</b>	Use the drop down list to display events by one of the following: <ul style="list-style-type: none"> <li>» Day</li> <li>» Week</li> <li>» Month</li> <li>» Year</li> <li>» Entire Period</li> </ul>
<b>Show importance</b>	Click the icons to display information according to importance. Available options are: <ul style="list-style-type: none"> <li>»  - Displays information events that do not normally contain important information.</li> <li>»  - Click to show Important events that need attention because they reflect important situations in the operation of GFI OneGuard Antivirus Agent.</li> <li>»  - Click to show events of critical importance that indicate problems in the operation of GFI OneGuard Antivirus Agent or vulnerabilities in protection of the user's computer.</li> </ul>

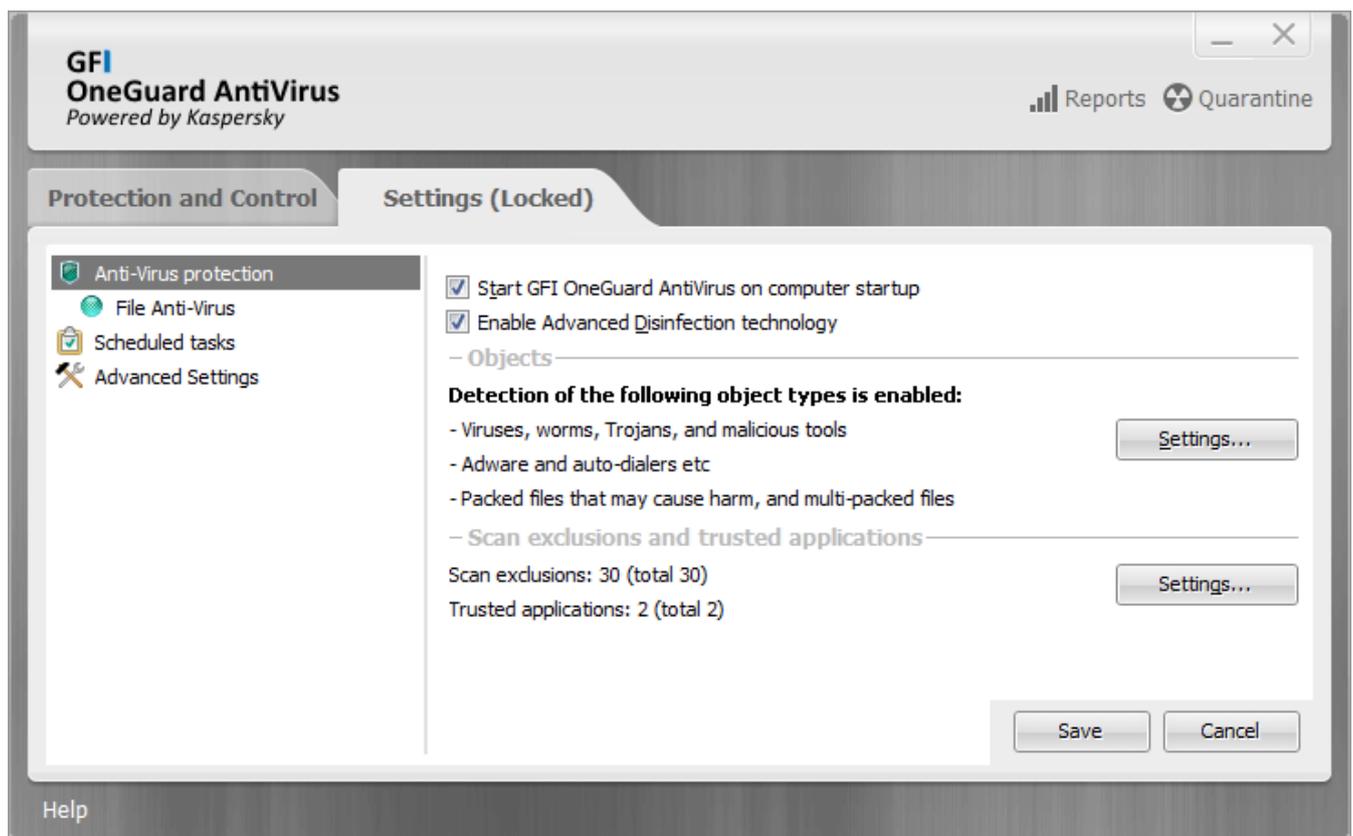
4. Click **Save report** to save a copy of the displayed information.
5. Select the character encoding of the report. Options are:
  - a. Save as ANSI
  - b. Save as Unicode
6. In the **Save as** window, specify the destination folder for the report file.
7. In the **File name** field, type the report file name.
8. In the **File type** field, select the necessary report file format: TXT or CSV.
9. Click **Save**.

## 2.6 Antivirus Agent settings

The Settings window shows application settings. Use these settings to review the configuration of the antivirus agent.

### IMPORTANT

The Antivirus Agent settings cannot be modified since these are centrally managed in GFI OneGuard by your administrator.



Screenshot 8: Antivirus protection settings

To open the Antivirus Agent Settings, right click the  icon in system tray and select **GFI OneGuard AntiVirus**. Click the **Settings** tab.

The left part of the Settings page contains application components, tasks, and other items. Select a node to display the applicable settings in the right pane.

Review the required settings. Since settings cannot be modified, contact your network administrator in case you would like to edit any settings.