GFI OneGuard™

END-USER GUIDE

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

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

Document Version: 2.0

Last updated (month/day/year): 04/10/2018

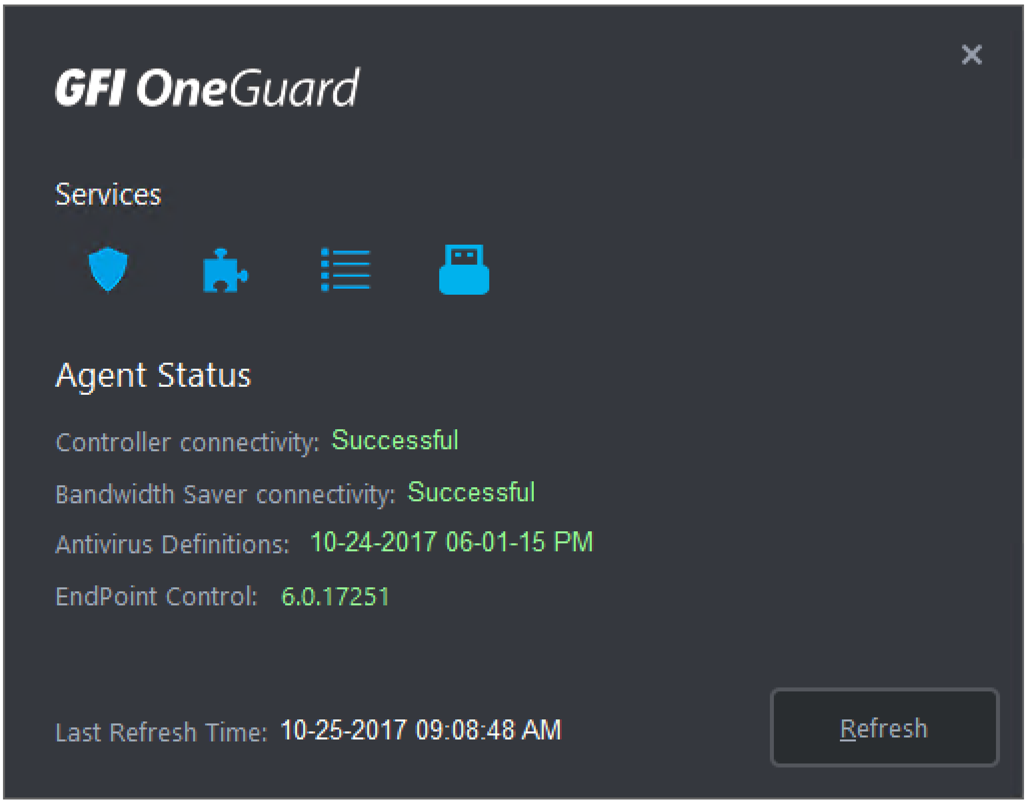
Contents

1 Introduction

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

This help system provides information to end-users on how to use the features available by the GFI OneGuard agent, including the antivirus agent and the EndPoint Control.

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.



Controller connectivity: Successful

Bandwidth Saver connectivity: Successful

Antivirus Definitions: 10-24-2017 06-01-15 PM

EndPoint Control: 6.0.17251

Last Refresh Time: 10-25-2017 09:08:48 AM

Screenshot 1: Monitoring the status of the GFI OneGuard Agent

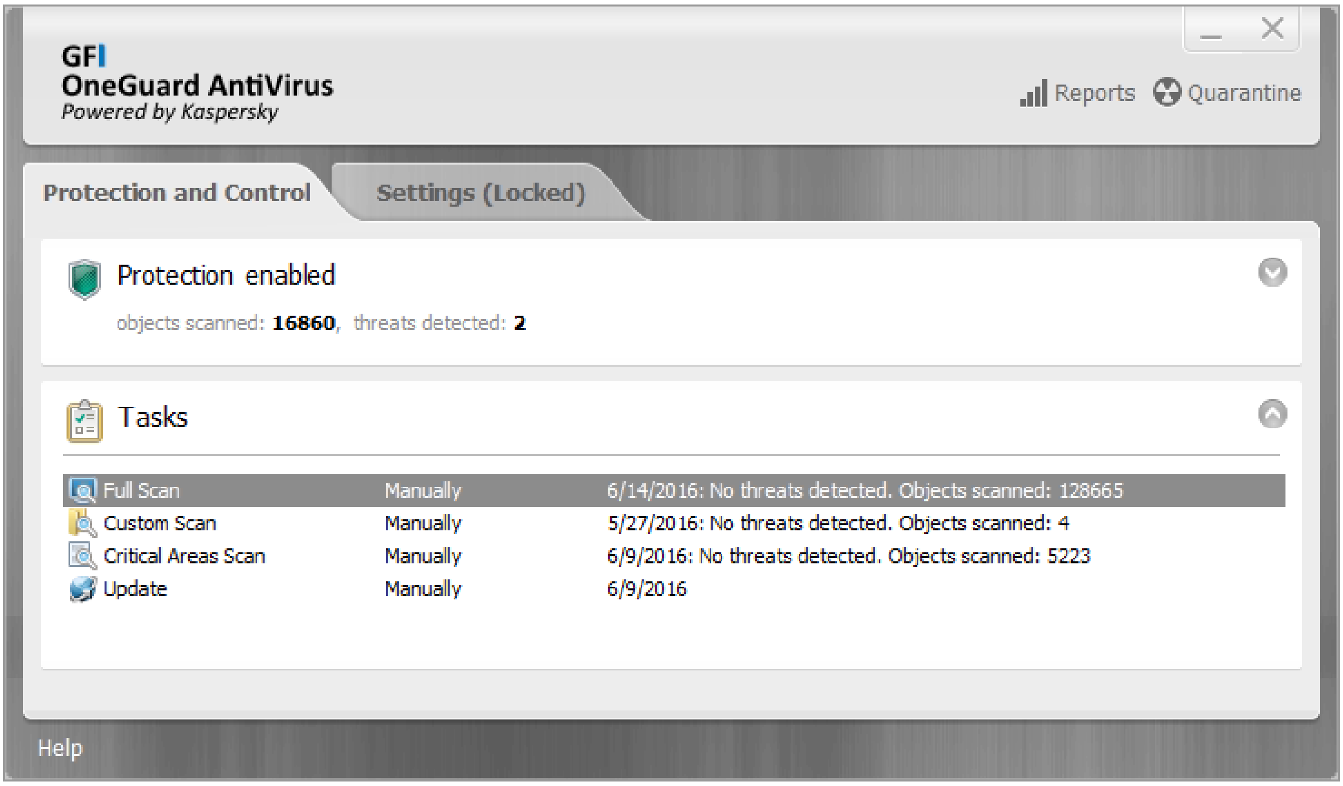
2 Using the Antivirus Agent

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.

POWERED BY KASPERSKY

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.



Protection enabled

objects scanned: **16860**, threats detected: **2**

Tasks

Full Scan	Manually	6/14/2016: No threats detected. Objects scanned: 128665
Custom Scan	Manually	5/27/2016: No threats detected. Objects scanned: 4
Critical Areas Scan	Manually	6/9/2016: No threats detected. Objects scanned: 5223
Update	Manually	6/9/2016

Screenshot 2: GFI OneGuard Antivirus Agent User Interface

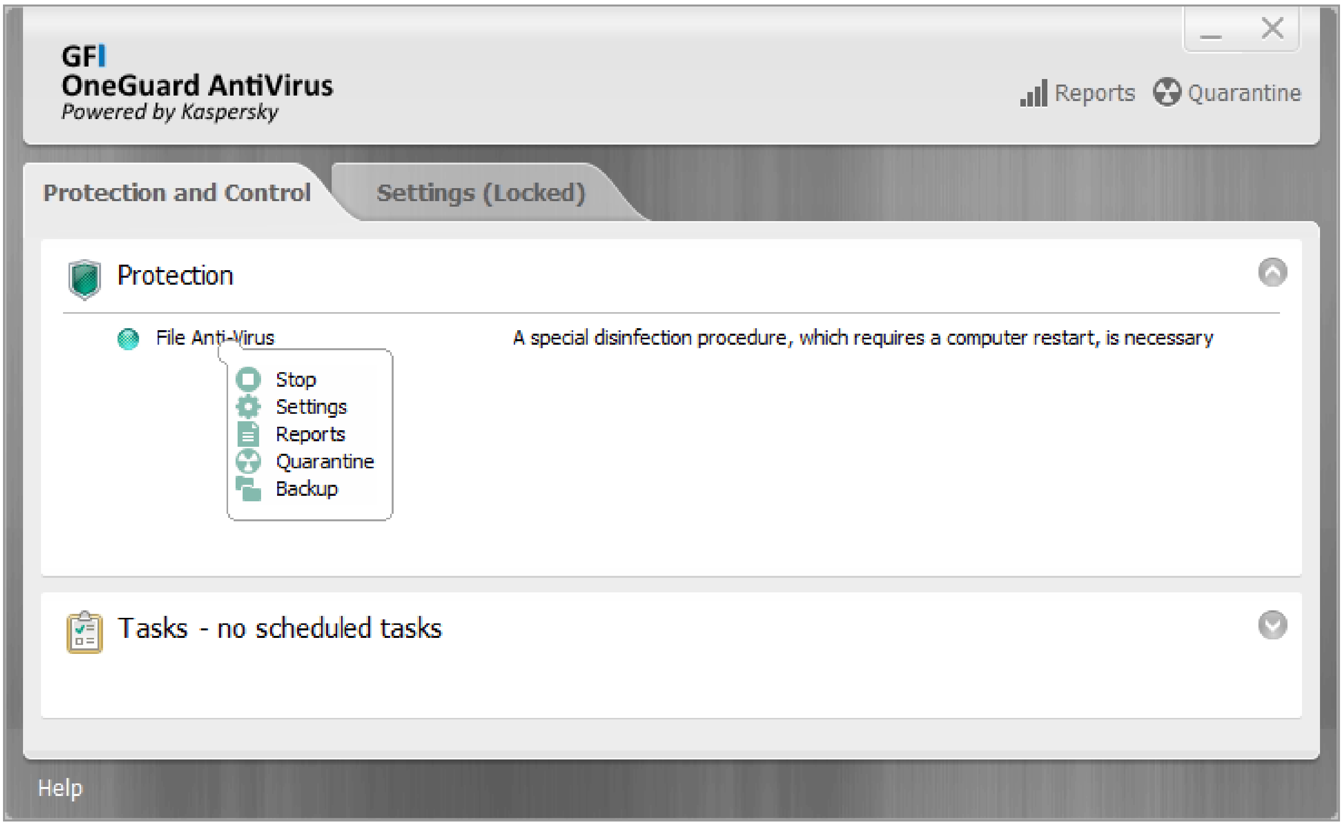
The main window of the Antivirus Agent contains the following elements:

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

Option	Description
Reports	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.
Quarantine	Review items that the antivirus agent detected as infected.
Unprocessed files	Information about files that the antivirus agent could not scan or process.
Backup	Access copies of files that were deleted or disinfected by the antivirus agent.
Help	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.



A special disinfection procedure, which requires a computer restart, is necessary

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
Protection	Shows the status of real time file protection (Active Protection) and any detected threats.

Section	Description
Tasks	A list of scans and tasks that can be triggered and their status. Click a task and choose the action to perform: » **Start scanning** - Starts an antivirus scan on the files that fall within the scope of the chosen scan type. » **Scan scope** - Select folders and files to be scanned by Antivirus Agent while performing the selected task. » **Start update** - Initiates an antivirus database and application module update task. » **Roll back update** - Reverts the application to the previous version of the update package. » **Settings** - Opens the settings of the selected component or task. Settings are not editable. For more information, refer to Antivirus Agent settings (page 12). » **Reports** - Opens a report on the events that occurred while a component or task was active. For more information, refer to Reports (page 10). » **Quarantine** - Opens the Quarantine area. For more information, refer to Quarantine (page 7). » **Backup** - Opens the Backup area. For more information, refer to Backup of malicious files (page 9). The following information is displayed for each task: » Task name » Task status » 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. » Statistics of the last instance of a task that has been completed. The statistics are shown on the right of the task status. » Error description, if the task completes with an error. The description is shown on the right of the task status.

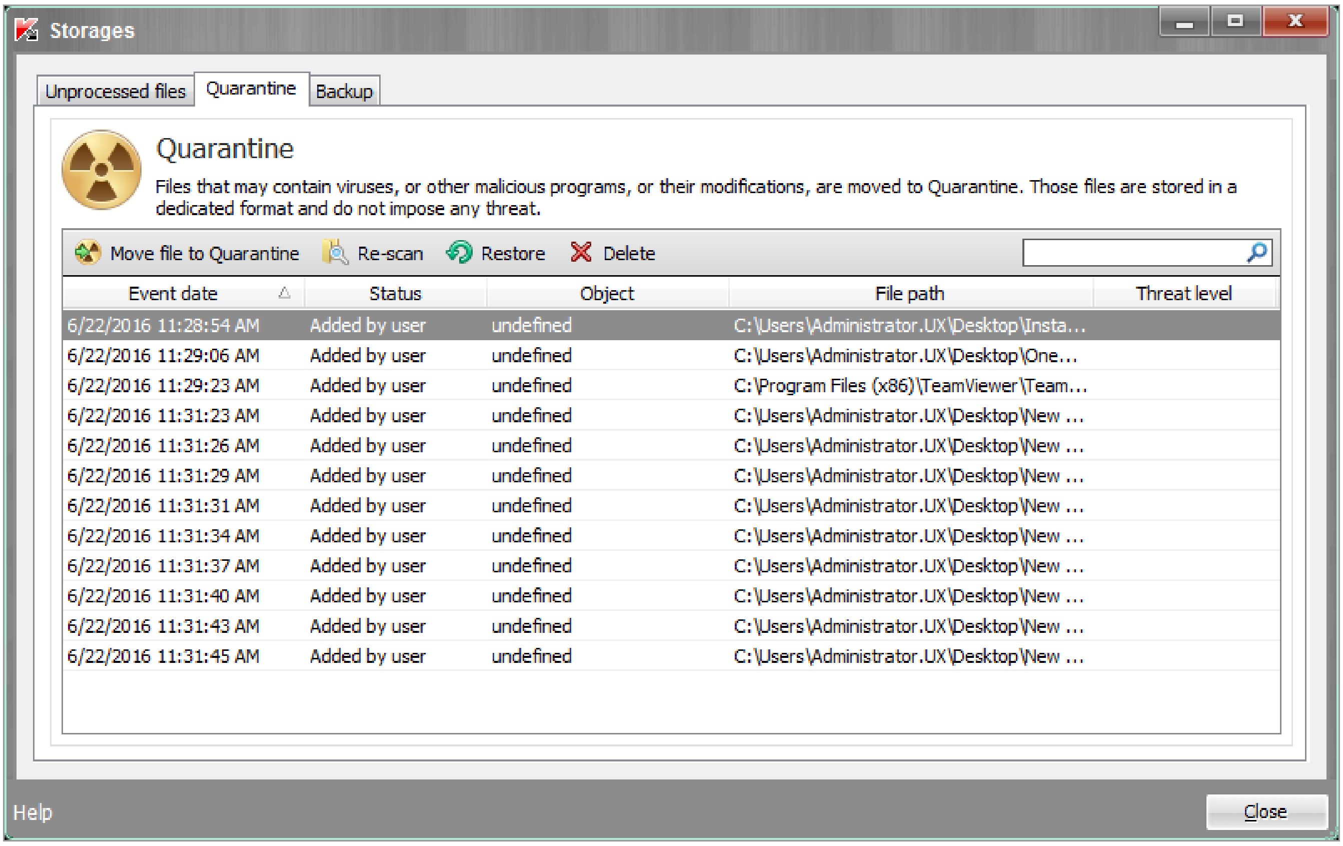
2.2 Quarantine

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).



Quarantine

Files that may contain viruses, or other malicious programs, or their modifications, are moved to Quarantine. Those files are stored in a dedicated format and do not impose any threat.

Event date	Status	Object	File path	Threat level
6/22/2016 11:28:54 AM	Added by user	undefined	C:\Users\Administrator.UX\Desktop\Insta...	
6/22/2016 11:29:06 AM	Added by user	undefined	C:\Users\Administrator.UX\Desktop\One...	
6/22/2016 11:29:23 AM	Added by user	undefined	C:\Program Files (x86)\TeamViewer\Team...	
6/22/2016 11:31:23 AM	Added by user	undefined	C:\Users\Administrator.UX\Desktop\New ...	
6/22/2016 11:31:26 AM	Added by user	undefined	C:\Users\Administrator.UX\Desktop\New ...	
6/22/2016 11:31:29 AM	Added by user	undefined	C:\Users\Administrator.UX\Desktop\New ...	
6/22/2016 11:31:31 AM	Added by user	undefined	C:\Users\Administrator.UX\Desktop\New ...	
6/22/2016 11:31:34 AM	Added by user	undefined	C:\Users\Administrator.UX\Desktop\New ...	
6/22/2016 11:31:37 AM	Added by user	undefined	C:\Users\Administrator.UX\Desktop\New ...	
6/22/2016 11:31:40 AM	Added by user	undefined	C:\Users\Administrator.UX\Desktop\New ...	
6/22/2016 11:31:43 AM	Added by user	undefined	C:\Users\Administrator.UX\Desktop\New ...	
6/22/2016 11:31:45 AM	Added by user	undefined	C:\Users\Administrator.UX\Desktop\New ...	

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:

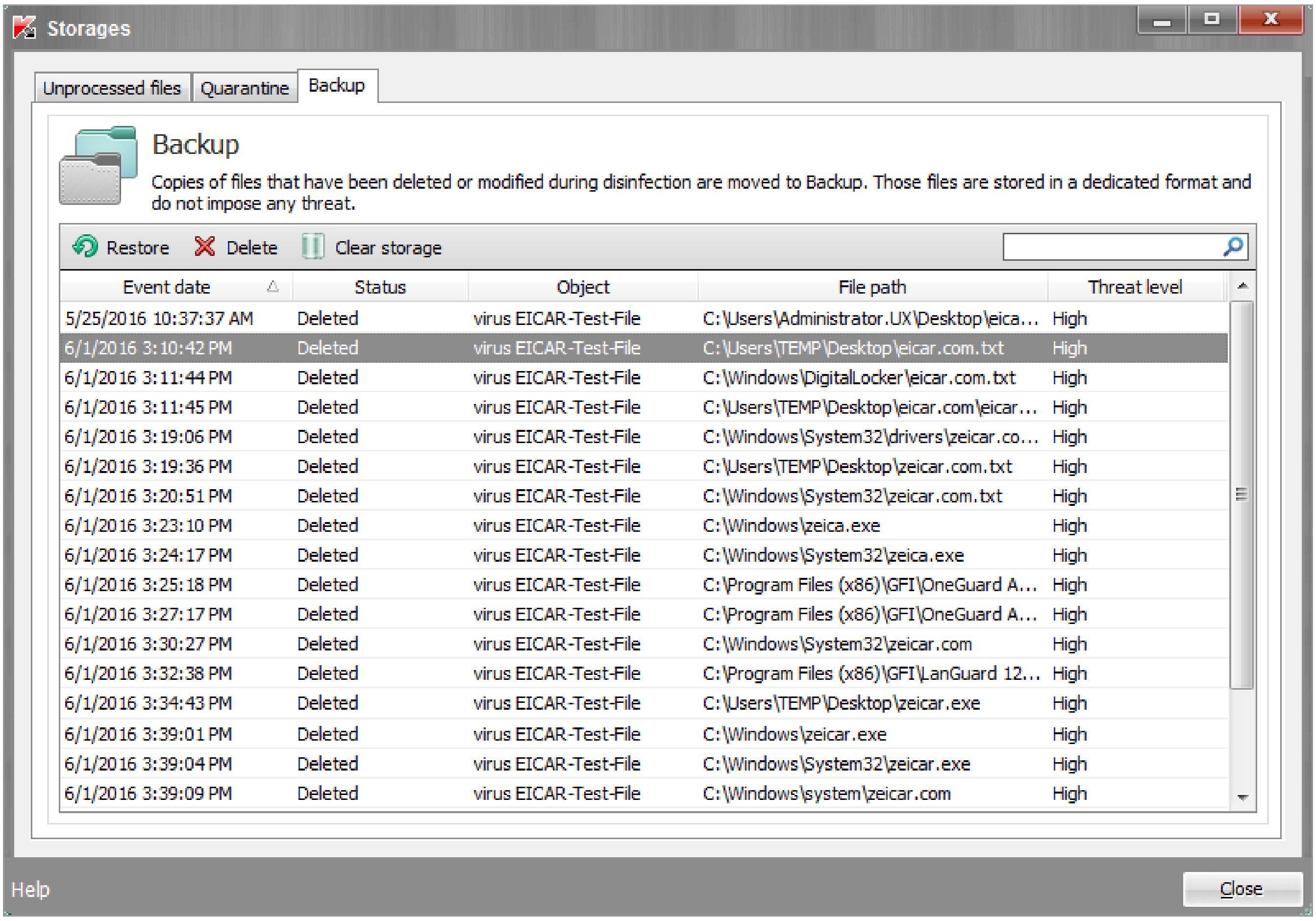
Action	Description
View quarantined files	The list of quarantined files is shown in the **Quarantine** tab.
Manually moving a file to Quarantine	You can manually quarantine a file that you suspect of containing viruses or other threats. To do this, click **Move file to Quarantine** and select the file to quarantine. Click **Open**. 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 **Re-scan** 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 **Restore all**. To restore one or more quarantined files, select one or more files to restore and click **Restore**. 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 **Delete**.

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.



Backup

Copies of files that have been deleted or modified during disinfection are moved to Backup. Those files are stored in a dedicated format and do not impose any threat.

Event date	Status	Object	File path	Threat level
5/25/2016 10:37:37 AM	Deleted	virus EICAR-Test-File	C:\Users\Administrator.UX\Desktop\eica…	High
6/1/2016 3:10:42 PM	Deleted	virus EICAR-Test-File	C:\Users\TEMP\Desktop\eicar.com.txt	High
6/1/2016 3:11:44 PM	Deleted	virus EICAR-Test-File	C:\Windows\DigitalLocker\eicar.com.txt	High
6/1/2016 3:11:45 PM	Deleted	virus EICAR-Test-File	C:\Users\TEMP\Desktop\eicar.com\eicar…	High
6/1/2016 3:19:06 PM	Deleted	virus EICAR-Test-File	C:\Windows\System32\drivers\zeicar.co…	High
6/1/2016 3:19:36 PM	Deleted	virus EICAR-Test-File	C:\Users\TEMP\Desktop\zeicar.com.txt	High
6/1/2016 3:20:51 PM	Deleted	virus EICAR-Test-File	C:\Windows\System32\zeicar.com.txt	High
6/1/2016 3:23:10 PM	Deleted	virus EICAR-Test-File	C:\Windows\zeica.exe	High
6/1/2016 3:24:17 PM	Deleted	virus EICAR-Test-File	C:\Windows\System32\zeica.exe	High
6/1/2016 3:25:18 PM	Deleted	virus EICAR-Test-File	C:\Program Files (x86)\GFI\OneGuard A…	High
6/1/2016 3:27:17 PM	Deleted	virus EICAR-Test-File	C:\Program Files (x86)\GFI\OneGuard A…	High
6/1/2016 3:30:27 PM	Deleted	virus EICAR-Test-File	C:\Windows\System32\zeicar.com	High
6/1/2016 3:32:38 PM	Deleted	virus EICAR-Test-File	C:\Program Files (x86)\GFI\LanGuard 12…	High
6/1/2016 3:34:43 PM	Deleted	virus EICAR-Test-File	C:\Users\TEMP\Desktop\zeicar.exe	High
6/1/2016 3:39:01 PM	Deleted	virus EICAR-Test-File	C:\Windows\zeicar.exe	High
6/1/2016 3:39:04 PM	Deleted	virus EICAR-Test-File	C:\Windows\System32\zeicar.exe	High
6/1/2016 3:39:09 PM	Deleted	virus EICAR-Test-File	C:\Windows\system\zeicar.com	High

Screenshot 5: GFI OneGuard Antivirus Backup area

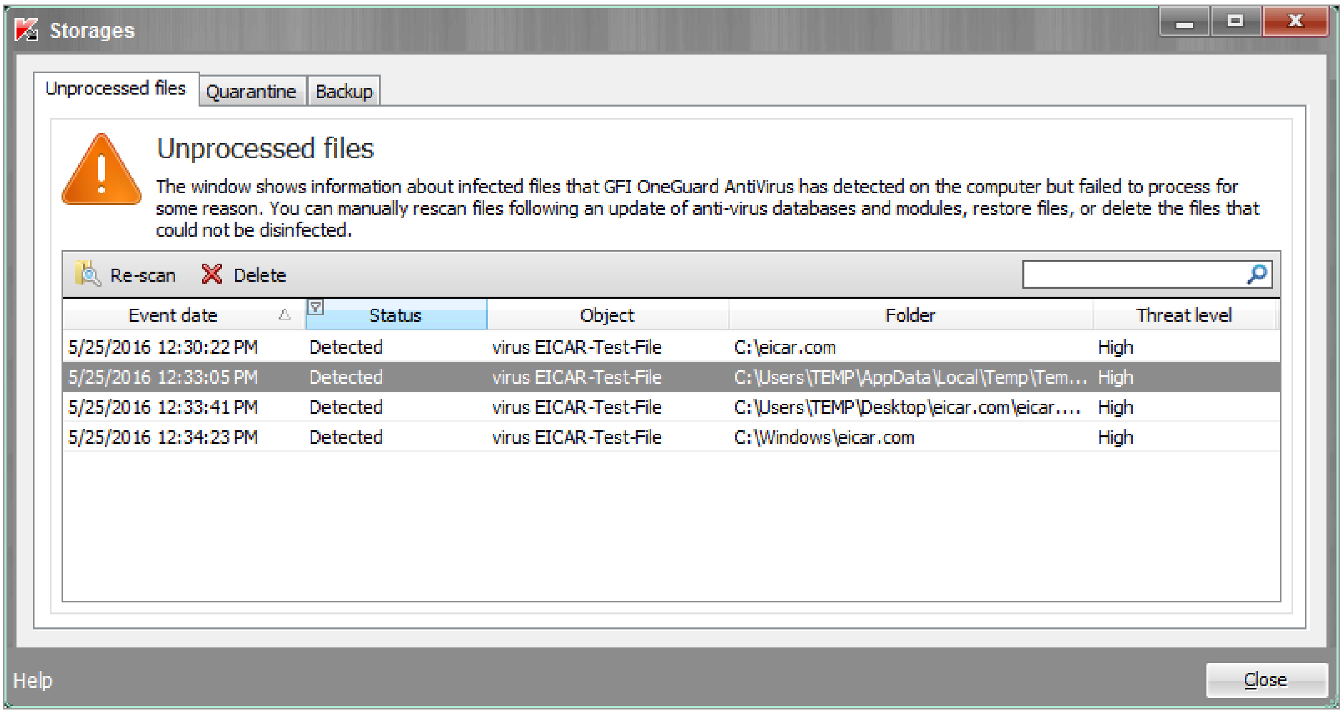
While managing Backup, you can perform the following actions with backup copies of files:

Action	Description
Restore files from backup copies to their original folders	Select one or more Backup events and click **Restore**. It is highly recommended to restore files only when they have a **Disinfected** 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 **Remove**.
Delete all backup copies	Click **Clear Storage** 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.



Unprocessed files

The window shows information about infected files that GFI OneGuard AntiVirus has detected on the computer but failed to process for some reason. You can manually rescan files following an update of anti-virus databases and modules, restore files, or delete the files that could not be disinfected.

Event date	Status	Object	Folder	Threat level
5/25/2016 12:30:22 PM	Detected	virus EICAR-Test-File	C:\eicar.com	High
5/25/2016 12:33:05 PM	Detected	virus EICAR-Test-File	C:\Users\TEMP\AppData\Local\Temp\Tem…	High
5/25/2016 12:33:41 PM	Detected	virus EICAR-Test-File	C:\Users\TEMP\Desktop\eicar.com\eicar.…	High
5/25/2016 12:34:23 PM	Detected	virus EICAR-Test-File	C:\Windows\eicar.com	High

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 **Re-scan**.
Delete unprocessed files	To delete unprocessed files, select one or more unprocessed files and click **Remove**.

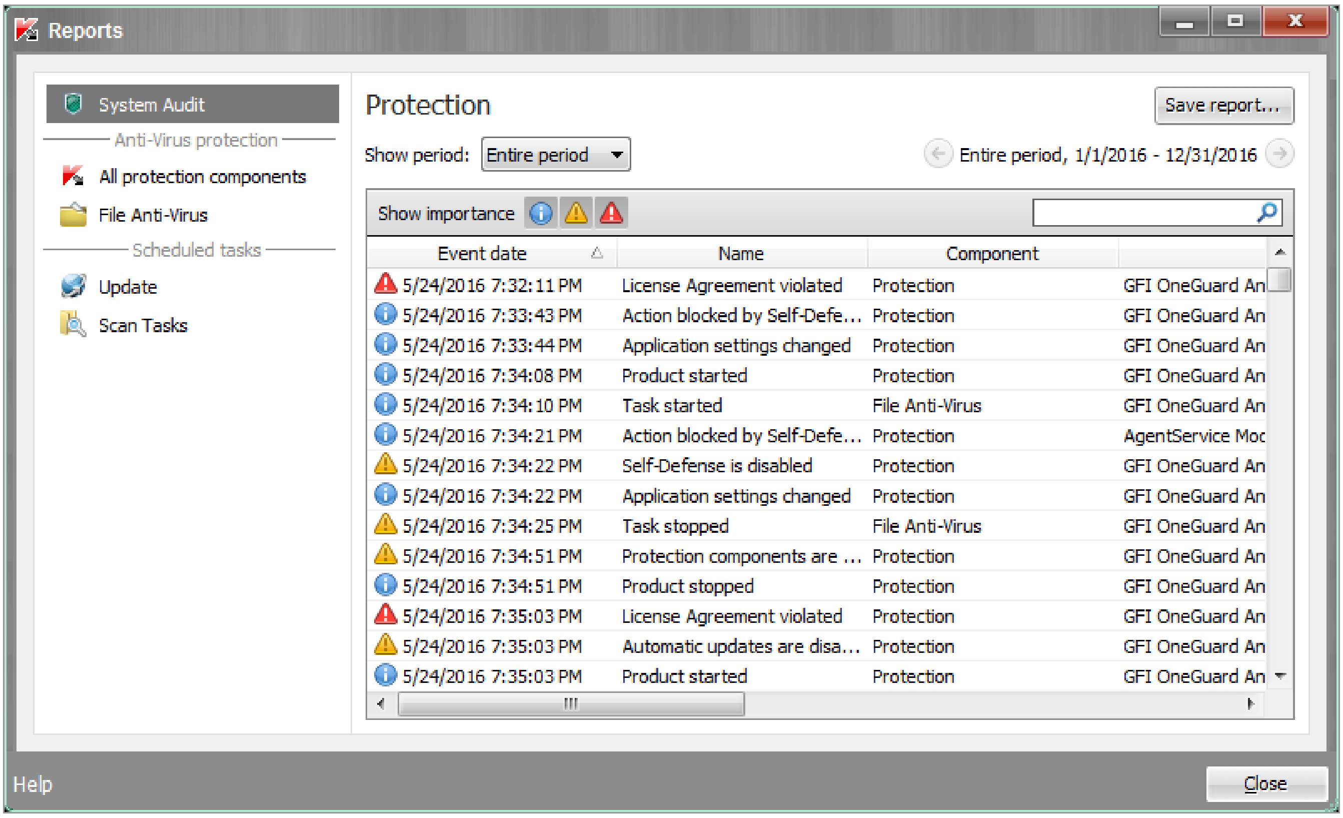
2.5 Reports

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**.



Reports

System Audit

Anti-Virus protection

All protection components

File Anti-Virus

Scheduled tasks

Update

Scan Tasks

Protection

Save report...

Show period: Entire period

Entire period, 1/1/2016 - 12/31/2016

Show importance ℹ ⚠ 🔺

	Event date	Name	Component	
🔺	5/24/2016 7:32:11 PM	License Agreement violated	Protection	GFI OneGuard An
ℹ	5/24/2016 7:33:43 PM	Action blocked by Self-Defe...	Protection	GFI OneGuard An
ℹ	5/24/2016 7:33:44 PM	Application settings changed	Protection	GFI OneGuard An
ℹ	5/24/2016 7:34:08 PM	Product started	Protection	GFI OneGuard An
ℹ	5/24/2016 7:34:10 PM	Task started	File Anti-Virus	GFI OneGuard An
ℹ	5/24/2016 7:34:21 PM	Action blocked by Self-Defe...	Protection	AgentService Moc
⚠	5/24/2016 7:34:22 PM	Self-Defense is disabled	Protection	GFI OneGuard An
ℹ	5/24/2016 7:34:22 PM	Application settings changed	Protection	GFI OneGuard An
⚠	5/24/2016 7:34:25 PM	Task stopped	File Anti-Virus	GFI OneGuard An
⚠	5/24/2016 7:34:51 PM	Protection components are ...	Protection	GFI OneGuard An
ℹ	5/24/2016 7:34:51 PM	Product stopped	Protection	GFI OneGuard An
🔺	5/24/2016 7:35:03 PM	License Agreement violated	Protection	GFI OneGuard An
⚠	5/24/2016 7:35:03 PM	Automatic updates are disa...	Protection	GFI OneGuard An
ℹ	5/24/2016 7:35:03 PM	Product started	Protection	GFI OneGuard An

Help

Close

Screenshot 7: GFI OneGuard Antivirus reports

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

Option	Description
System Audit	Contains information about events occurring during the interaction between the user and the application and in the course of application operation in general.
All Protection Components	Information about events that are logged in the course of operation of the GFI OneGuard Antivirus Agent.
File Antivirus	Contains information about events that occur during the operation of the File Antivirus component.
Update	Click to view only update tasks.
Scan Tasks	Click to view a list of scan tasks.
Show period	Use the drop down list to display events by one of the following: » Day » Week » Month » Year » Entire Period
Show importance	Click the icons to display information according to importance. Available options are: » ℹ - Displays information events that do not normally contain important information. » ⚠ - Click to show Important events that need attention because they reflect important situations in the operation of GFI OneGuard Antivirus Agent. » 🔺 - 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.

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.

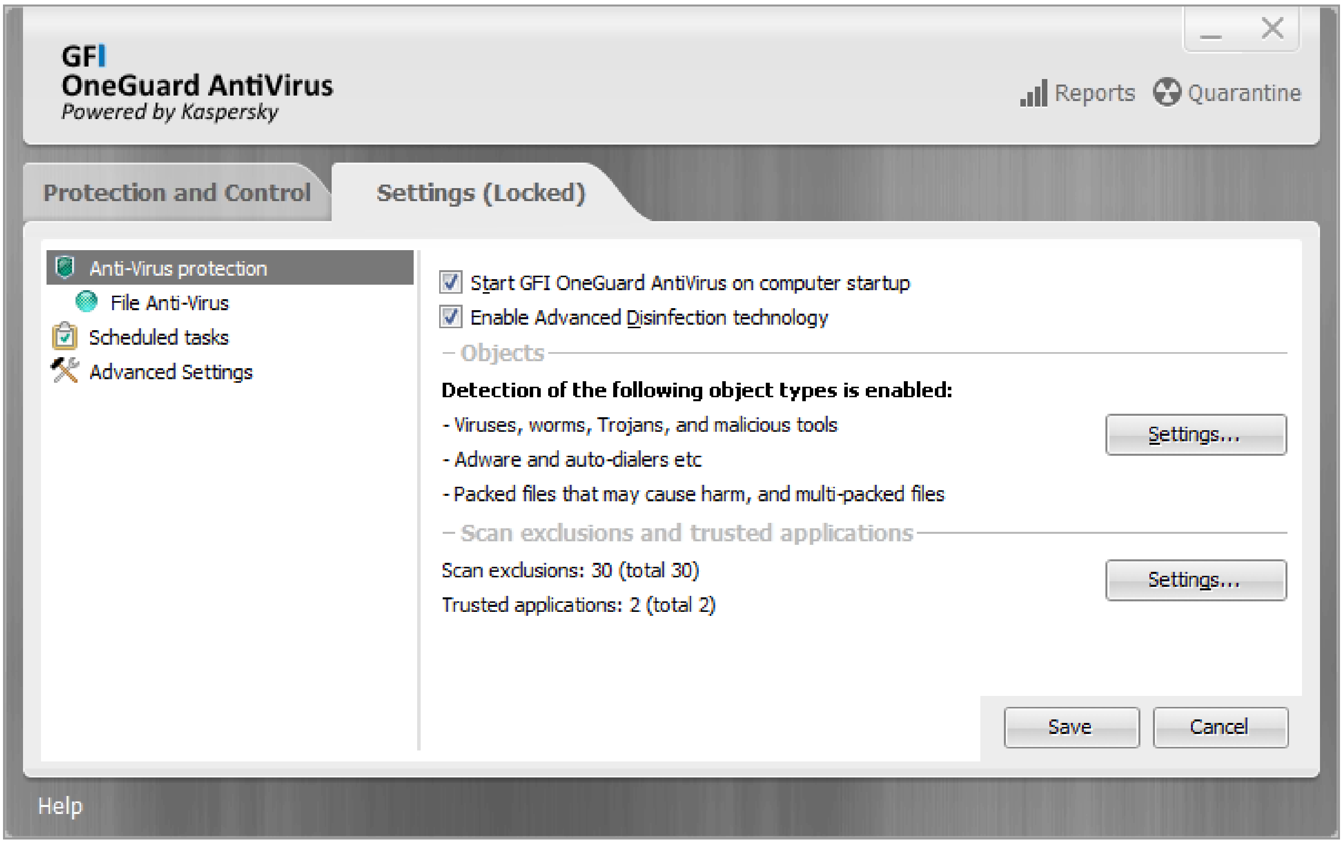
8. In the **File type** field, select the necessary report file format: TXT or CSV.

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.



☑ Start GFI OneGuard AntiVirus on computer startup

☑ Enable Advanced Disinfection technology

Objects

Detection of the following object types is enabled:

- Viruses, worms, Trojans, and malicious tools
- Adware and auto-dialers etc
- Packed files that may cause harm, and multi-packed files

Scan exclusions and trusted applications

Scan exclusions: 30 (total 30)

Trusted applications: 2 (total 2)

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.

3 EndPoint Control

GFI OneGuard offers network users extended protection over available devices.

Policies may block the access to certain devices or file types. When access to a device attached to a computer is blocked, contact an administrator.

EndPoint Control also offers the possibility to request temporary access to blocked devices. Users can request a limited time access to a device that is blocked by a policy.

Encryption is another feature of EndPoint Control. When a policy enforces encryption of a USB device, the user must enter a password to start the encryption process.

Topics in this section:

3.1 Temporary Access

EndPoint Control enables users to request temporary access to blocked devices. This enables users to access devices and connection ports on protected target computers for a specified time window.

The request for temporary access has three steps:

1. The user requests temporary access to a protected device.

2. The administrator generates an unlock code and sends it to the user.

3. The user enters the unlock code into the Temporary Access form.

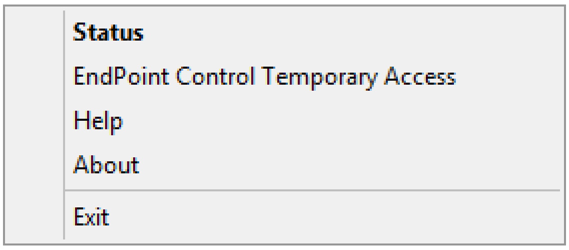
This topic covers only the steps that require user intervention.

Step 1: Requesting temporary access to a protected device

The first step is to obtain a temporary access code from the device:

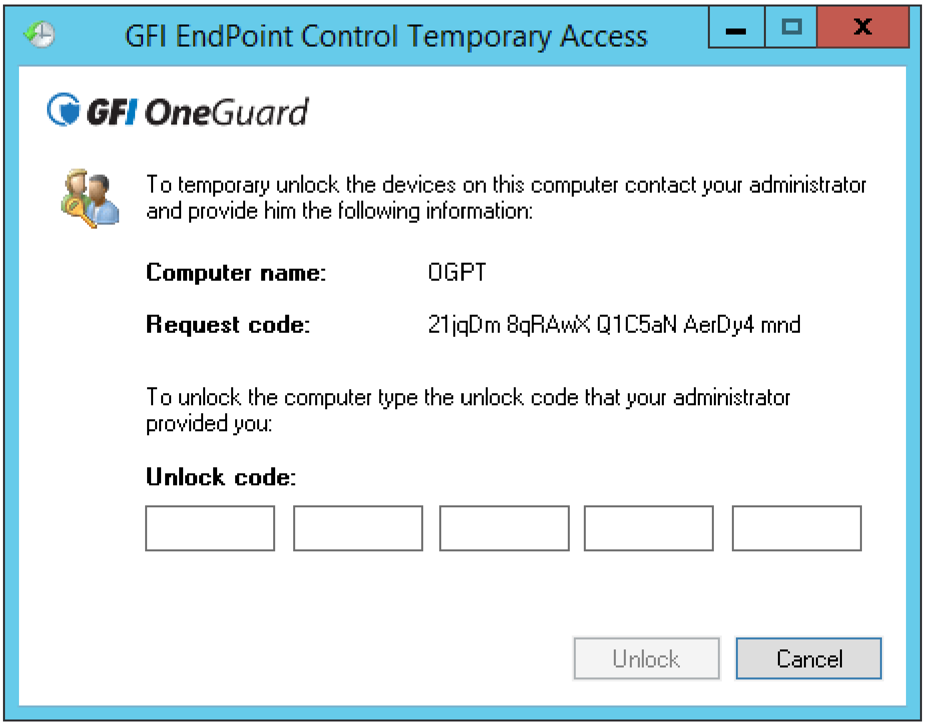
1. Login on the computer you want to request access.

2. From the computer tray, right-click the GFI OneGuard agent icon .



Screenshot 9: Options of the OneGuard agent.

3. Click **EndPoint Control Temporary Access**.



To temporary unlock the devices on this computer contact your administrator and provide him the following information:

Computer name: OGPT

Request code: 21jqDm 8qRAwX Q1C5aN AerDy4 mnd

To unlock the computer type the unlock code that your administrator provided you:

Unlock code:

Screenshot 10: Temporary Access request form

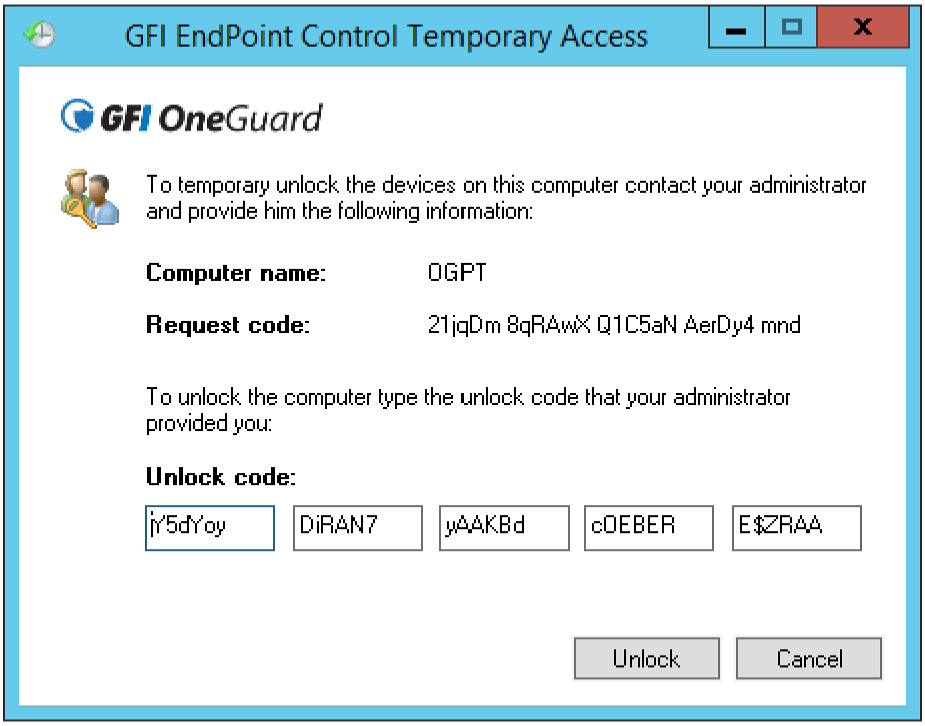
4. Copy the **Request code** string and send it to the administrator together with the machine name.

Step 2: Entering the Unlock Code into the device

Once the administrator sends back the Unlock code, insert it into the GFI EndPoint Control Temporary Access window.

To insert the unlock code:

1. From the computer tray, right-click the GFI OneGuard agent icon .
2. Click **EndPoint Control Temporary Access**.



To temporary unlock the devices on this computer contact your administrator and provide him the following information:

Computer name: OGPT

Request code: 21jqDm 8qRAwX Q1C5aN AerDy4 mnd

To unlock the computer type the unlock code that your administrator provided you:

Unlock code: jY5dYoy DiRAN7 yAAKBd cOEBER E$ZRAA

Screenshot 11: Unlock code inserted into the Temporary Access window.

3. Insert the code sent by the administrator under **Unlock code**.

4. Click **Unlock**.

3.2 Encryption

EndPoint Control offers GFI OneGuard administrators the ability to enable volume encryption.

When volume encryption is enforced, users must provide a password to encrypt and access a storage device's data.

Passwords are an important part of the security system. A good password should be easy to remember but difficult for others to guess. A strong password should have a combination of upper and lower cases, numbers and symbols.

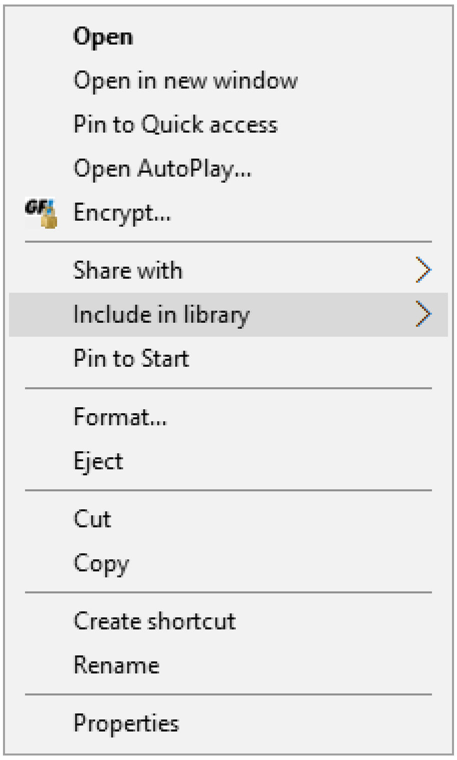
The following actions can be performed:

- Enabling encryption
- Removing encryption
- Changing password
- Using the Traveler Application

Enabling encryption

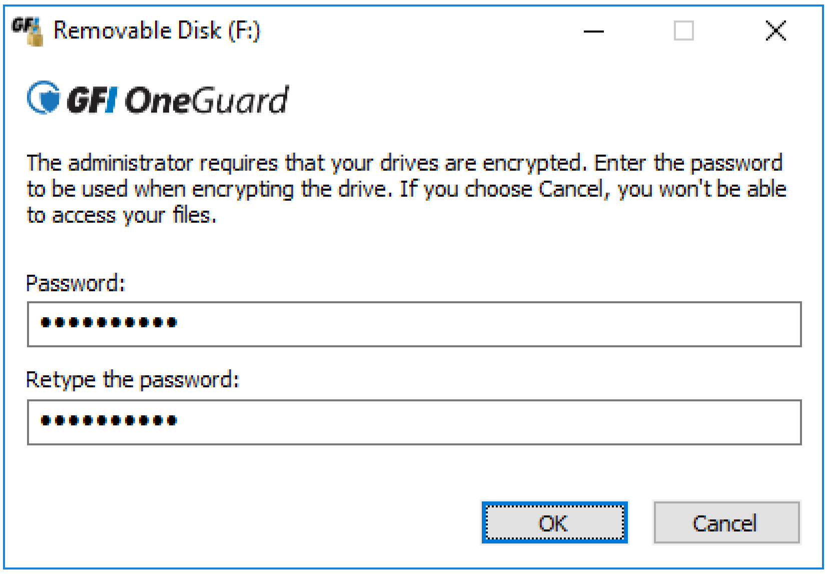
To start encryption:

1. Insert the device into the drive.



Screenshot 12: Option to activate encryption

2. Right-click the USB drive and click **Encrypt...**.



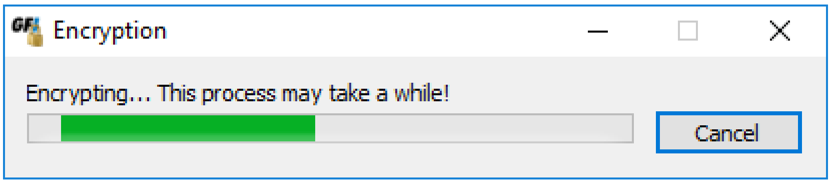
The administrator requires that your drives are encrypted. Enter the password to be used when encrypting the drive. If you choose Cancel, you won't be able to access your files.

Password: ••••••••••

Retype the password: ••••••••••

Screenshot 13: Enabling encryption

3. Key in the **Password** and **Retype the password** to confirm.



Encrypting... This process may take a while!

Screenshot 14: Encryption bar progress

The process may take several minutes depending on the size of the drive. Once the process is complete, the device is ready for use.

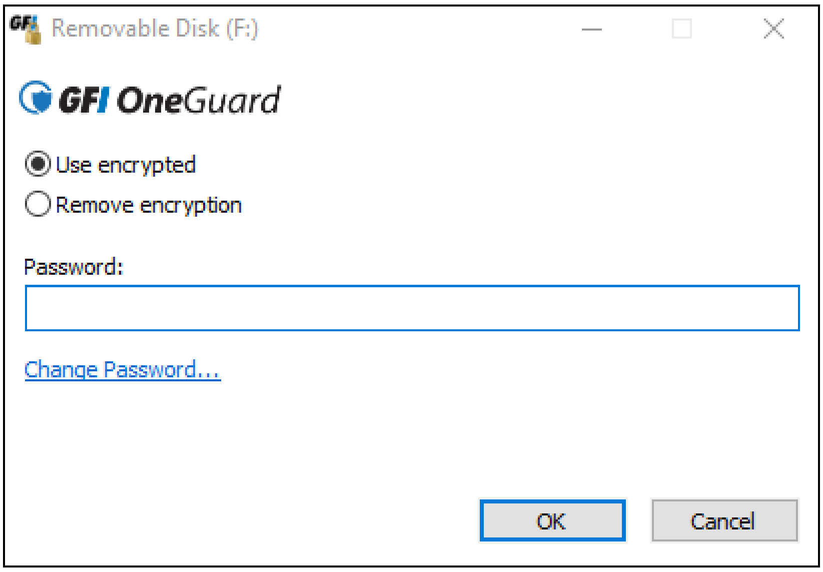
Each time the device is re-inserted in the drive the user must enter the password again.

Removing the encryption

Encryption can be removed at any time. Be aware that a device cannot be used on a machine that has encryption enabled. The procedure can be useful if you need to use the device in a computer that is not protected by GFI OneGuard EndPoint Control and the traveler application is not enabled.

To remove encryption follow these steps:

1. Insert the device into the drive.



● Use encrypted
○ Remove encryption

Password:

Screenshot 15: Options available when inserting the device

2. Select **Remove encryption** and enter the **Password**.

EndPoint Control starts the process and and prompts on completion that decryption was disabled.

Changing the password

If you need to change the password for the encryption, follow these steps:

1. Insert the device in the drive.

2. Click **Change Password...**.

3. Type in the following information:

Fields	Description
Current password	Key-in the password used when encrypting the device.
New password	Key-in a new password.
Retype the new password	Retype to confirm the password.

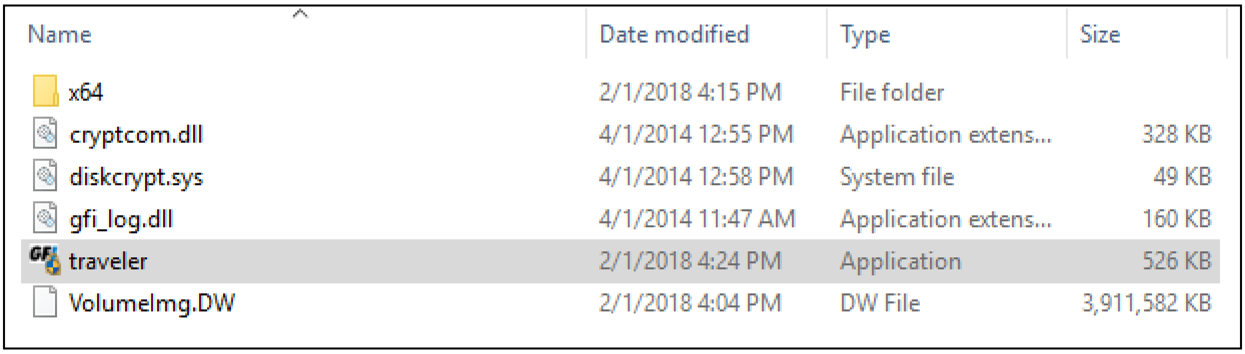
4. Click **Save**.

Remove and re-insert the device for the new prompt for the password.

Using the Traveler Application

By default, a device encrypted by GFI OneGuard EndPoint Control can only be decrypted by devices using the same agent.

An exception is when the policy for the device enables the Traveler application. Traveler enables you to decrypt data encrypted by GFI OneGuard on storage devices from computers that are not running a GFI OneGuard Agent.



Name	Date modified	Type	Size
x64	2/1/2018 4:15 PM	File folder	
cryptcom.dll	4/1/2014 12:55 PM	Application extens...	328 KB
diskcrypt.sys	4/1/2014 12:58 PM	System file	49 KB
gfi_log.dll	4/1/2014 11:47 AM	Application extens...	160 KB
traveler	2/1/2018 4:24 PM	Application	526 KB
VolumeImg.DW	2/1/2018 4:04 PM	DW File	3,911,582 KB

Screenshot 16: Encrypted drive with the traveler application

When this option is enabled, during the encryption process the Traveler app is installed on the device. Then, when inserting the device in a machine that does not have the EndPoint Control agent, the user gets the same prompt for the password used with the agent.

To start the traveler application:

1. Insert the device into the drive of a machine that does not have the EndPoint Control agent.

2. Navigate the content of the drive and double-click **traveler**.

3. Enter the password used to encrypt the device.

A second driver appears and the content of the driver is available.