Malwarebytes
ANTI-RANSOMWARE

Malwarebytes Anti-Ransomware Administrator Guide

Version 0.9

21 March 2017

Malwarebytes

Notices

CWB23-0091b

Table of Contents

What is Ransomware?

In the simplest terms, the name *ransomware* says it all. It is a method by which your files are hijacked, encrypted, and held for ransom by attackers until you pay the ransom. If you wait too long, the price goes up. Wait longer, and you lose the opportunity to pay the ransom and lose your files in the process. If that worries you, it should!

How Malwarebytes Protects Against Ransomware

Ransomware is a type of malware, and because of the danger which it presents, it receives a lot of attention. It often arrives on your endpoint because of unpatched or little-known vulnerabilities which are exploited by attackers. Some applications are so attack-prone that users elect not to use them. If the vulnerability is in the operating system, users have few choices available to them. Patches and updates are released to counter the vulnerabilities, but there is no guarantee that eliminating old vulnerabilities will not create new ones. Malwarebytes uses a multi-layer approach to protect your endpoints against the threat of ransomware.

The average user may be a target for any or all of these threats at any given time. It does not matter which websites they frequent, or which emails they open. Threats exist, so protection is warranted.

Businesses face a greater threat of attack. Intellectual property and financial information are but two types of information which attackers want. The attackers may be competitors, foreign governments, identity thieves, anarchists or simply a computer-savvy person with a grudge. They will use whatever methods at their disposal to mine their targets for information. These include phishing, social engineering, malvertising, probing networks for weaknesses, and back-door access through unsuspecting business partners. The list of reasons goes on forever, as does the list of methods that attackers use.

As long as attackers have a motive to launch threats against a business or consumer computer, they will do that. They will also continue to become more effective in that process. We believe everyone has a fundamental right to a malware-free existence. Our mission is to create the best disinfection and protection solutions to combat the world's most harmful Internet threats. Our mission never stops!

You can learn more about Malwarebytes security technologies at http://www.malwarebytes.com/business/.

System Requirements

Following are minimum requirements for an endpoint on which *Malwarebytes Anti-Ransomware* may be installed. Please note that these requirements do not include any other functionality that the endpoint is responsible for.

Hardware Requirements

- **Operating System:** Windows 10 (32/64-bit), Windows 8.1 (32/64-bit), Windows 8 (32/64-bit), Windows 7 (32/64-bit)
- **CPU:** 800 MHz or faster
- **RAM:** 1024 MB
- **Free Disk Space:** 100 MB
- **Recommended Screen Resolution:** 1024x768 or higher
- **Active Internet connection**

External Access Requirements

If your company's Internet access is controlled by a firewall or other access-limiting device, you must grant access for *Malwarebytes Anti-Ransomware* to reach Malwarebytes services. These are:

https://data.service.malwarebytes.org	Port 443	outbound
https://data-cdn.mbamupdates.com	Port 443	outbound
https://keystone.mwbsys.com	Port 443	outbound

Please note: These URLs may not be configured to respond to pings.

Installation

IMPORTANT NOTES:

NOTE 1: We recommend that you deploy *Malwarebytes Anti-Ransomware* in stages. Begin with a small number of endpoints in a controlled environment, then add additional departments/endpoint groups until installation is complete on all endpoints. Unsigned applications are at a higher risk of being categorized as a *false positive* (legitimate file judged to be malicious). This deployment method allows exclusions to be added where needed.

NOTE 2: If you have been using the *Malwarebytes Anti-Ransomware* beta client, you must uninstall it before beginning installation of the current version.

After downloading *Malwarebytes Endpoint Security*, you will find two *Malwarebytes Anti-Ransomware* installers in the `\Unmanaged\Windows\` directory. These files are:

- `MBARW_Business_Setup.msi`
- `MBARW-Business_Setup.exe`

GUI Installation

To begin the installation, double-click on the *Malwarebytes Anti-Ransomware* installation file which you downloaded. If you are installing *Malwarebytes Anti-Ransomware* on a Windows version newer than Windows XP, a dialog box will be displayed in the center of your screen, labeled **User Account Control**. Verify that the publisher is Malwarebytes Corporation and click **Yes**. Once approved, installation will begin. The installation program will display several screens to guide you through the installation, and allows you to provide alternate information if you do not wish to accept installation defaults. Each screen will also allow you to terminate installation if you do not wish to continue. Screens are as follows:

- **Setup Preparation:** This screen requests that you close all other applications, and temporarily disable both your anti-virus program and firewall program before continuing.
- **License Agreement:** You must accept the terms of the license agreement if you wish to continue installation.
- **Information Panel:** A change log is presented in the form of an information panel.
- **Select an Installation Directory:** In most cases, you can simply click **Next** to accept the default location. **Please note** that the amount of free disk space required for the program is listed at the bottom of this screen. You should assure that you have sufficient disk space for the program as well as for program logs.
- **Select a Start Menu Folder** (optional)**:** Links to start *Malwarebytes Anti-Ransomware* will be stored here.
- **Ready to Install:** A final confirmation is required from you to perform the installation.
- **Installation Complete:** You may also launch *Malwarebytes Anti-Ransomware* at this time.

At this point, program installation is complete.

MSI Silent Installation

The msi file is designed for use by the Microsoft Package Installer (msiexec), while the second file can be installed in the Windows GUI by double-clicking on it, or on the Windows command line. To install using msiexec, the specific command is shown below. Please note that the command is not case-sensitive.

```
msiexec /i MBARW_Business_Setup.msi /quiet
```

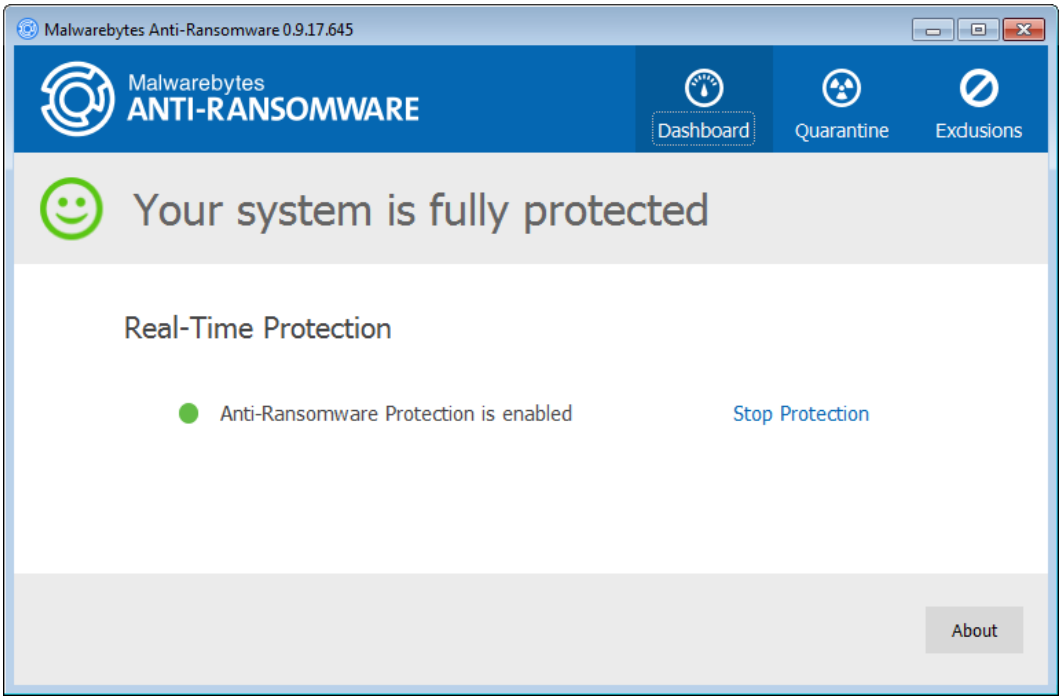
EXE Silent Installation

If you wish to install the exe file from the Windows command line, begin by loading an administrative command prompt (right-click on **Command Prompt** and select Run as Administrator). Navigate to the directory where the installer is located, and enter the following command.

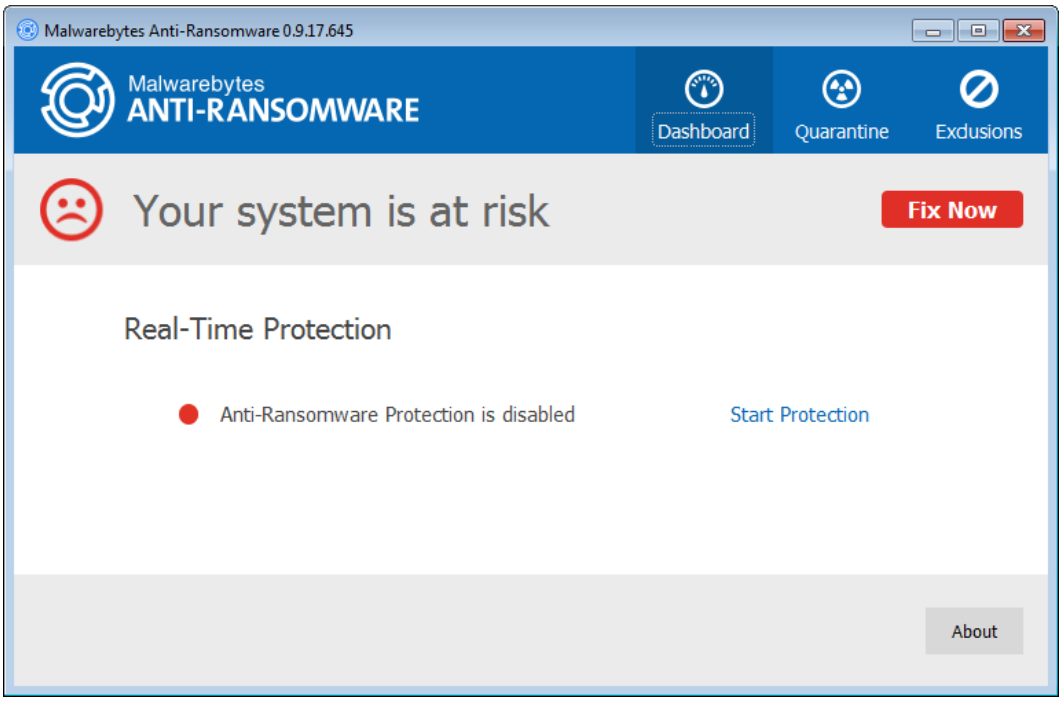
```
MBARW-Business_Setup.exe /SP- /verysilent /suppressmsgboxes
```

Dashboard

The view shown is the Dashboard. Clicking the *Dashboard* button from any other screen will lead you back to this screen. Its primary purpose is to inform you of program status. As shown here, *Malwarebytes Anti-Ransomware* is fully functional and protecting your system.

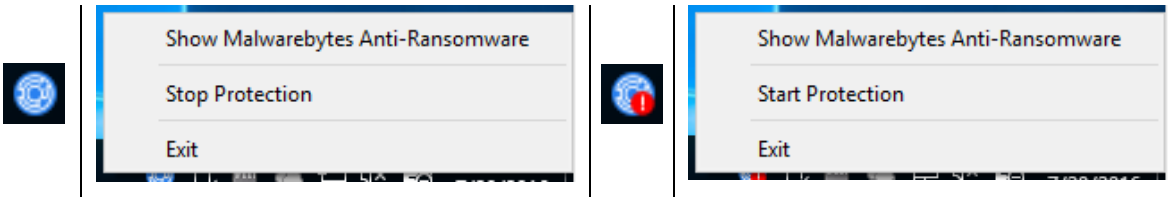


The next screenshot shows what you would see if you clicked the **Stop Protection** link.



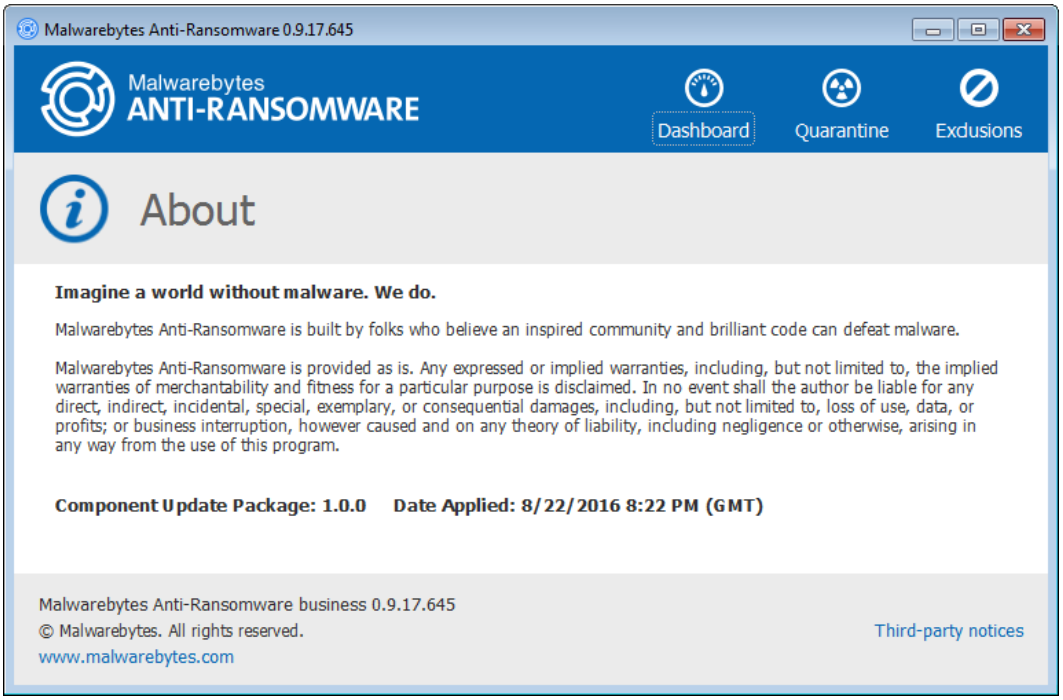
Both the banner and the status message have changed, and the **Fix Now** button is clearly shown in the banner.

Program status is also shown in the system tray, usually at the bottom left corner of your screen. That location may be different if you elected to show it elsewhere. When the program is running properly, you will see the icon shown at the left. You may right-click the icon to bring up a context menu as shown here. This allows you to stop ransomware protection, show the program interface (if it had been minimized), or exit the application completely. If you stop protection, the icon will now show a red exclamation point to indicate there is an issue with your protection. The context menu here will allow you to restart protection.



About screen

In the bottom right corner of the screen is the About button. When clicked, it takes you to the screen shown below.

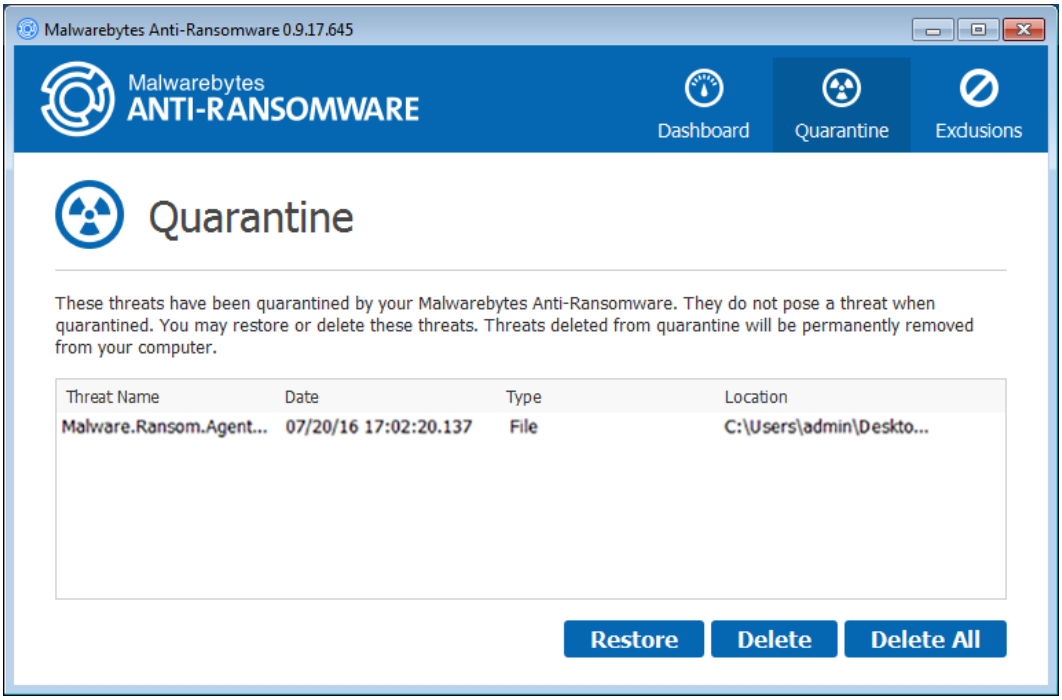


Should you have the need to call for technical support on the anti-ransomware client, you may be asked for information which is shown on this screen.

Quarantine

Any files categorized as ransomware are accessible to the user on the Quarantine screen. Information about each file is presented to assist you in determining whether it should be deleted. Once categorized as a potential threat, it is modified to prevent it from performing any malicious activity, and then moved to Quarantine. Three action buttons are provided. These allow you to restore individual files to their original unmodified condition (and to their original location on your file system), delete individual files, or delete all files. Restoring a file is a once-only action, and will not prevent that file from appearing in Quarantine at a later time.

A screenshot of the Quarantine screen is shown here.

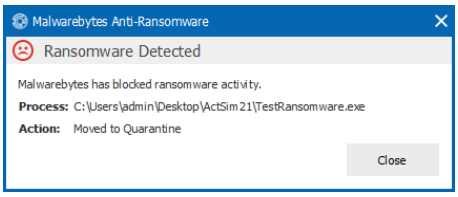


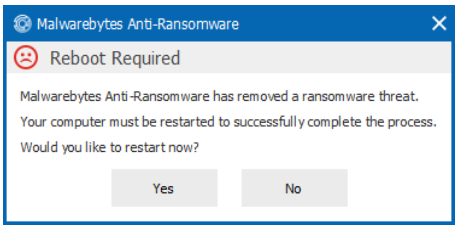
Please Note: That there may be files categorized as ransomware which are actually not malicious. This is referred to as a *false positive*. Detection methods are not foolproof, and we prefer to err on the side of caution to provide the best possible protection for our users.

To delete or restore a file from Quarantine, click the file to select it, then click the button corresponding to your desired action. To perform this operation on multiple files, click the first file, then shift-click to select a contiguous group of files, or ctrl-click on each file to be acted upon, then click the button corresponding to your desired action.

Notifications

If a file has been categorized as ransomware by *Malwarebytes Anti-Ransomware*, it will be moved to Quarantine and you will be notified in the lower right corner of your screen. A sample notification is shown below in the screenshot to the left.

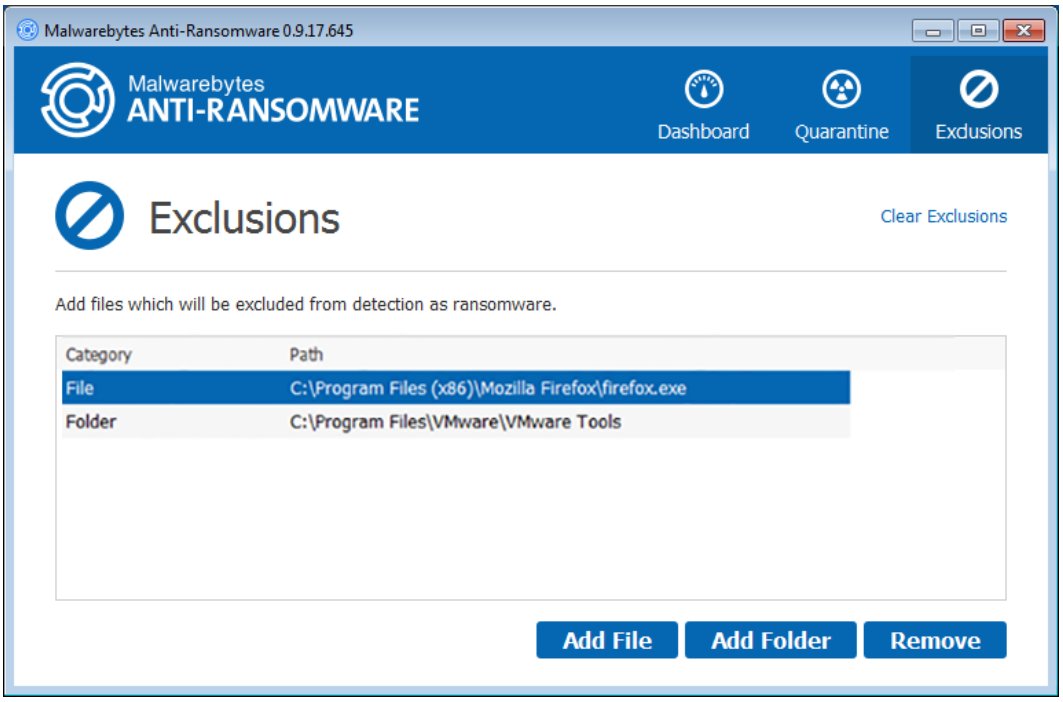




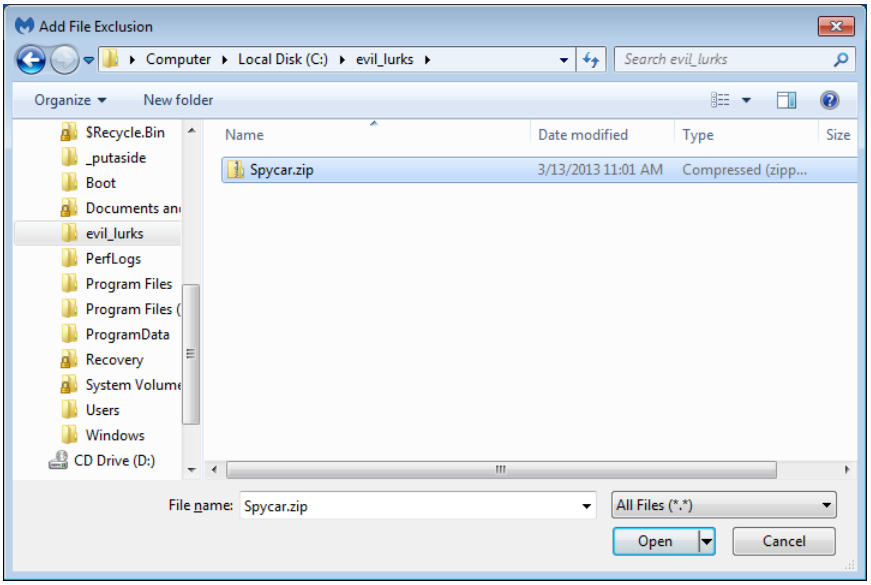
We must assume that if ransomware activity was present on the endpoint, the possibility exists for damage caused by memory-resident malware which could survive even if the file which contained the malware was safely removed. For this reason, the endpoint should be rebooted to assure that the ransomware – in all possible forms – has been removed. A screenshot of that notification message is shown above in the screenshot to the right.

Exclusions

This screen allows you to specify files and folders to be excluded from analysis by *Malwarebytes Anti-Ransomware*. As mentioned in the previous section, a file which is restored after appearing in Quarantine will continue to be quarantined unless and until it is listed as an exclusion. You will not want to exclude a file out of convenience, as that file may be malicious. You should only exclude a file if you know and trust the file.

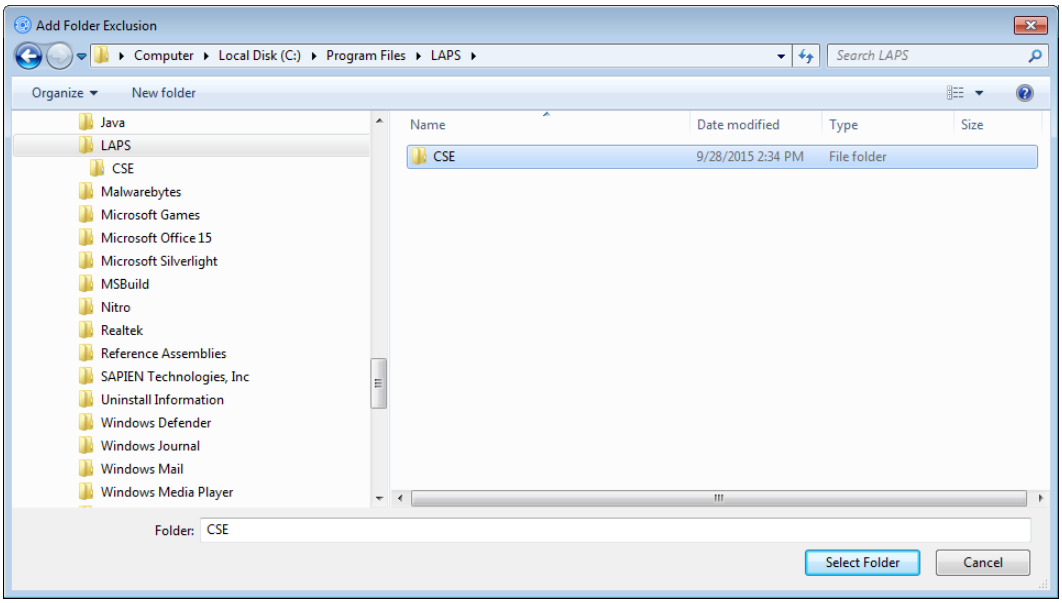


You may add a file or folder to the Exclusions list, using a selection window click the Add File button to launch the *Add File Exclusion* window as shown below.



If you wish to exclude multiple files within a single directory, you must exclude each individually. You may exclude as many files as you wish, but they must be specified individually. Once specified, the file(s) will appear in the Exclusion List in the main window. **Please note** that the dimensions of this window have been modified from the size that the window opens to initially. This was

done for clarity of presentation here. You may modify the size of this window to suit your needs as well. You may also add an exclusion for a folder. This type of exclusion would typically be added if you know and trust every file in the folder, and there was no chance for any file in that directory to be a carrier of ransomware.



To remove a file from the Exclusions list, click the file to select it, then click Remove. To remove multiple files, click the first file, then shift-click to select a contiguous group of files, or ctrl-click on each file to be removed from the list, then click Remove. To remove all files from the Exclusion list, click the Clear Exclusions link.

Appendix A: Command Line Reference Guide

Malwarebytes Anti-Ransomware utilizes a second executable (*assistant.exe*) to pass a limited set of command line parameters. The command line structure uses actions and modifiers. Actions are specified with a double hyphen ("––"). Modifiers are specified in plain text, and must be separated from actions by spaces. Modifiers which include embedded spaces must be surrounded by double quote characters. In addition, the following conventions are used:

- Required specifications are encased by angle brackets
  Example: **assistant <––action> <modifier>**
- Choice of modifiers are separated by vertical bars
  Example: **assistant <––action> <modifier_1|modifier_2>**

Commands listed here are primarily used by a system administrator via script, batch file, GPO updates, or remote desktop. In certain instances, the admin has configured *Malwarebytes Anti-Ransomware* to operate as a task which is invisible to the user. When this is the case, command line tools offer the only method of modifying program configuration on the endpoint.

Protection

This command starts or stops anti-ransomware protection on the endpoint.

Usage:

assistant <––protection | ––p> <*parameter*>

Purpose:

This command starts or stops anti-ransomware protection on the endpoint. The action <*protection*> may also be represented by <*p*>.

Modifier:

<*parameter*> Valid modifiers for this command are **start** and **stop**.

Examples:

assistant --protection start
assistant --p stop

Exclusions

This command allows exclusions to be added or deleted from ransomware analysis.

Usage:

assistant <––exclusions | ––x> add <*parameter*>
assistant <––exclusions | ––x> delete-all

Purpose:

This command allows exclusions to be added or deleted from ransomware analysis. An added exclusion is a file which will not be tested as potential ransomware. An exclusion which has been deleted will be tested as a potential source of ransomware.

Parameters:

<*parameter*> A file or folder which will be excluded from testing. If the file/folder contains embedded spaces, the file/folder should be surrounded by double quotes so that the full string is excluded as intended.

Examples:

assistant ––exclusions add c:\safe_executable.exe	*Exclude a file*
assistant ––x add "c:\work files\safe_executable.exe"	*Exclude a file (embedded space in folder name)*
assistant ––exclusions delete-all	*Delete all exclusions*

Quarantine

This command allows quarantined files to be restored on the file system, or permanently deleted.

Usage:

assistant <––quarantine | ––q> restore <*parameter*>
assistant <––quarantine | ––q> delete-all
assistant <––quarantine | ––q> restore-all

Purpose:

This command allows quarantined files to be restored on the file system, or permanently deleted. Restored files will behave as normal files prior to their quarantining, and will be subject to testing as a possible source of ransomware.

Parameters:

<*parameter*> A file which should be restored on the file system. The file will be subject to testing as a source of ransomware unless it is added to exclusions.

Examples:

assistant ––quarantine add c:\safe_executable.exe	Q*uarantine a file*
assistant ––q add "c:\work files\safe_executable.exe"	Q*uarantine a file (embedded space in folder name)*
assistant –– quarantine delete-all	*Delete all quarantined files*
assistant –– quarantine restore-all	*Restore all quarantined files to the file system*