# Malwarebytes Anti-Malware Remediation Tool
# Administrators Guide

Version 1.0

18 August 2014

Malwarebytes

# Notices

This document is provided "as-is."  The information contained in this document is subject to change without notice and is not warranted to be error-free.  If you find any errors, we would appreciate your comments; please report them to us in writing.

# Contents

# 1.0 Getting Started

*Malwarebytes Anti-Malware Remediation Tool* is a portable product, designed to allow business users to detect and remove malware from endpoints. It combines the power of our flagship anti-malware product (*Malwarebytes Anti-Malware*) and our cutting edge *Chameleon* technology, which allows *Malwarebytes Anti-Malware Remediation Tool* to run in environments which often render other anti-malware applications helpless.

*Malwarebytes Anti-Malware* is considered to be the next step in the detection and removal of malware. We have compiled a number of new technologies that are designed to quickly detect, destroy, and prevent malware. *Malwarebytes Anti-Malware* can detect and remove malware that even the most well-known antivirus and antimalware applications on the market today cannot.

Implementation in a portable form provides increased flexibility for IT staff to quickly and easily deploy the product, use it to remediate threats, gather logs, and continue with their daily tasks – all without a large investment in time or resources.

## 1.1 Key Features

*Malwarebytes Anti-Malware Remediation Tool* offers the following key features:

- Three different types of scans to analyze your endpoint for malware threats, regardless of whether they are based in memory, file system or registry.
- Ability to perform full scans for all drives.
- Ability to utilize Malwarebytes database updates, assuring that even the newest threats can be detected.
- Intelligent heuristics to analyze potential threats when they are designed to evade signatures.
- Ability to quarantine detected threats, and to selectively restore on demand.
- Ability to deploy product to endpoints using your preferred methods.
- Command line capabilities allow IT staff to modify certain program configuration settings, execute scans, and gather logs through integration with customer-supplied scripts, batch files, and group policy updates.
- Product leaves no lasting footprint on endpoint.
- *Chameleon* technology allows *Malwarebytes Anti-Malware Remediation Tool* to clean your endpoints even when malware blocks other anti-malware software.

## 1.2 System Requirements

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

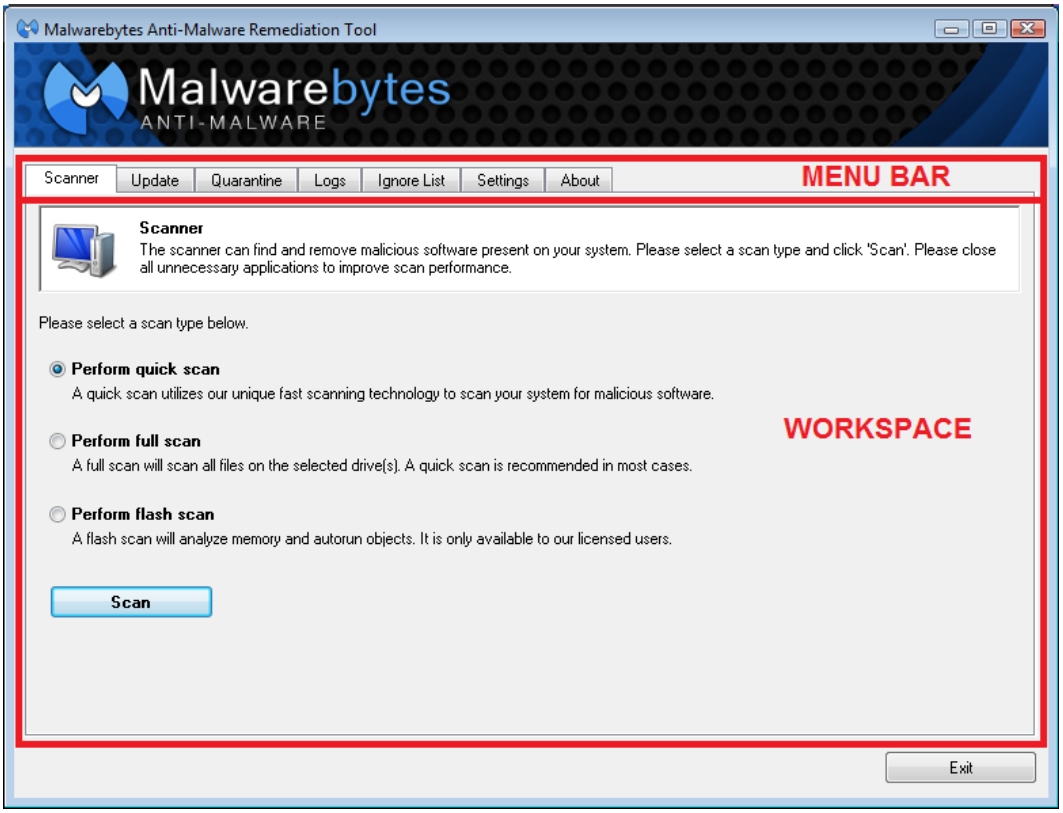
- **Operating System:** Windows 8.1 (32/64-bit), Windows 8 (32/64-bit), Windows 7 (32/64-bit), Windows Vista (32/64-bit), Windows XP (Service Pack 2 or later, 32-bit only)
- **CPU:** 800 MHz or faster
- **RAM:** 256 MB (512 MB or more recommended)
- **Free Disk Space:** 20 MB
- **Screen Resolution:** 800x600 or higher
- **Active Internet Connection**
- **Internet Browser**
- **USB 2.0 Port** (optional, depending on deployment method)

## 2.0 Using Malwarebytes Anti-Malware Remediation Tool

This section of the guide discusses each program screen, and provides guidance for everyday operation. It is important to note that while all program functionality is available within the user interface, the program also supports interaction via a command line. This is useful when considering that the program may be executed both locally and remotely. A user typically interacts locally, and would use the graphical interface for that purpose. IT staff would likely deploy and execute remotely. It is more convenient for them to use the command line for their needs. The command line interface will be discussed later in this guide. For now, let's look at the user interface.

## 2.1 Screen Layout

All functionality offered by *Malwarebytes Anti-Malware Remediation Tool* occurs through the interface shown below. The two major regions of the user interface are shown here, bounded by red borders. The **Menu Bar** provides interactive access to the seven primary functional areas of the program. Selecting any tab changes the information displayed in the **Workspace** region.



Scanner

The scanner can find and remove malicious software present on your system. Please select a scan type and click 'Scan'. Please close all unnecessary applications to improve scan performance.

Please select a scan type below.

● Perform quick scan
A quick scan utilizes our unique fast scanning technology to scan your system for malicious software.

○ Perform full scan
A full scan will scan all files on the selected drive(s). A quick scan is recommended in most cases.

○ Perform flash scan
A flash scan will analyze memory and autorun objects. It is only available to our licensed users.

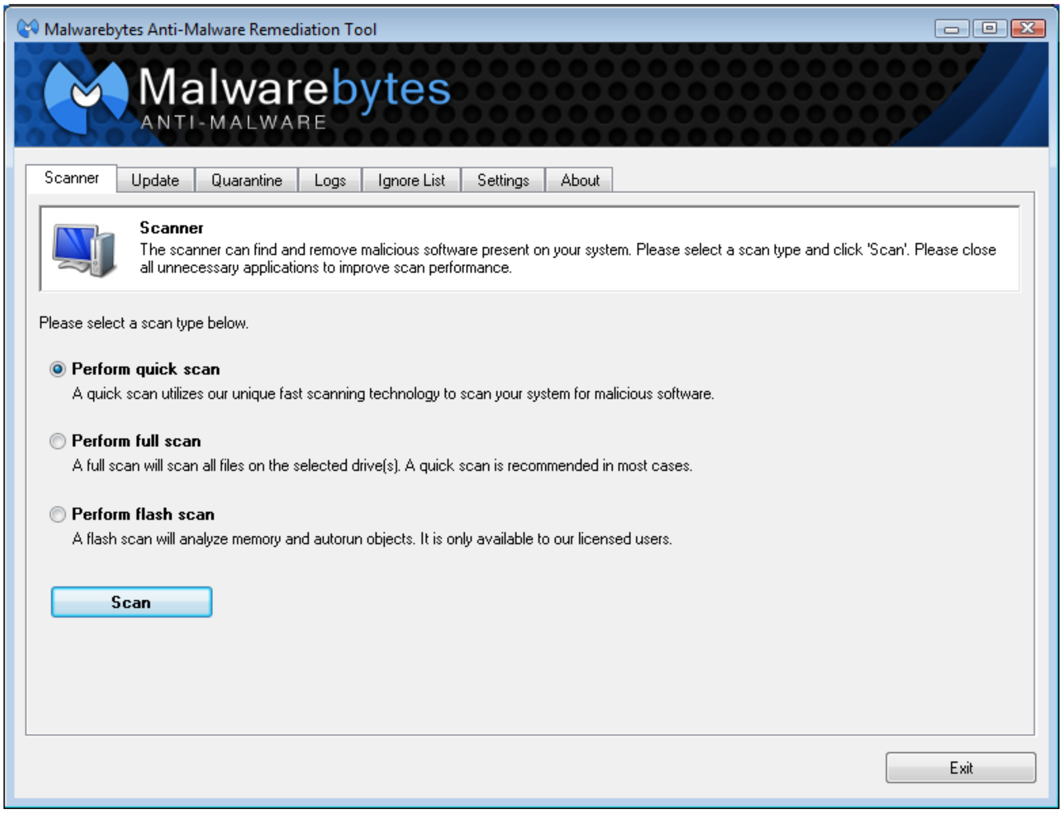
The purpose of each tab on the **Menu Bar** is as follows:

- **Scanner:** Selects a scan type and executes it.
- **Update:** Provides status of signature database, and enables on-demand update.
- **Quarantine:** Management of quarantined threats.
- **Logs:** Access to logs containing scan results
- **Ignore List:** Management of items which will be ignored during scanning.
- **Settings:** Detailed configuration of program, scanner and database updater.
- **About:** Program version, license, and link to on-line help.

As each tab is selected, its background color will change from gray to white. The **Workspace** is then used for functionality associated with the selected tab.

## 2.2 Scanner Tab

This tab provides the capability to select a method of scanning, and to execute the selected scan. A screenshot is shown below.



**Scanner**

The scanner can find and remove malicious software present on your system. Please select a scan type and click 'Scan'. Please close all unnecessary applications to improve scan performance.

Please select a scan type below.

● **Perform quick scan**
A quick scan utilizes our unique fast scanning technology to scan your system for malicious software.

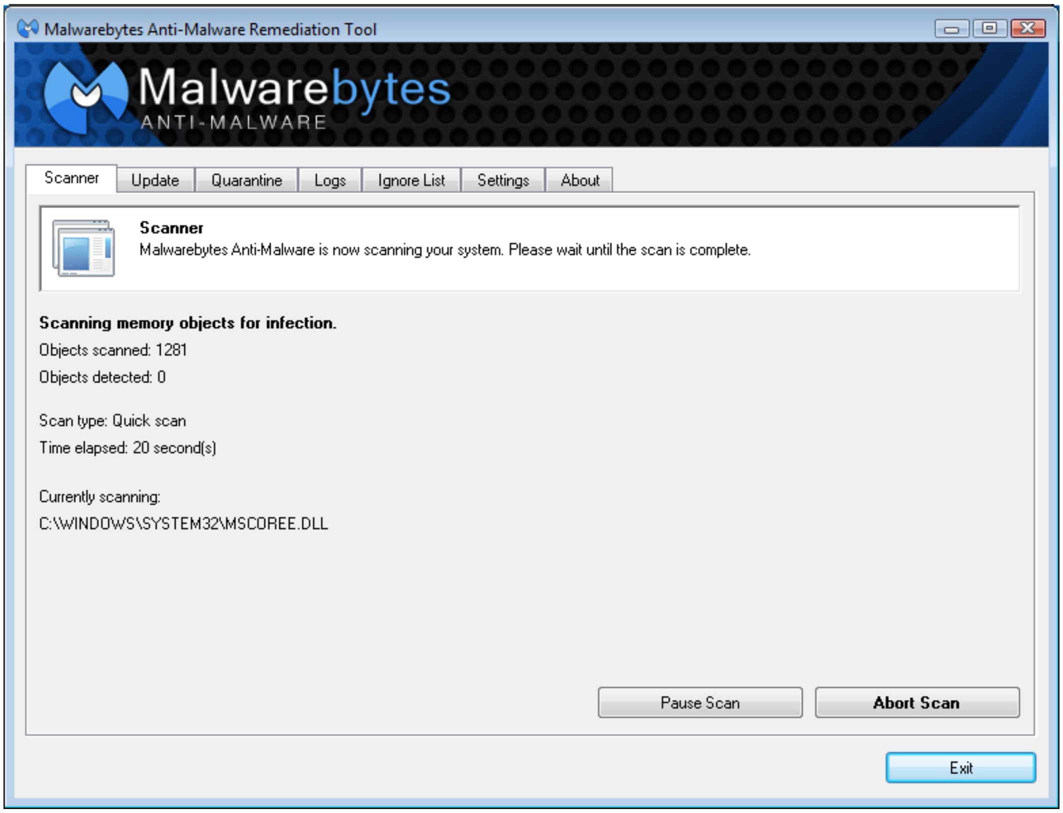
○ **Perform full scan**
A full scan will scan all files on the selected drive(s). A quick scan is recommended in most cases.

○ **Perform flash scan**
A flash scan will analyze memory and autorun objects. It is only available to our licensed users.

*Malwarebytes Anti-Malware Remediation Tool* offers three methods of scanning an endpoint. They are:

- **Quick Scan:** Scans all system locations where malware is known to install itself. This is the method recommended by Malwarebytes.
- **Full Scan:** Scans all files on selected drive(s). The option to select drives becomes available once the **Scan** button has been clicked. In most cases, a **Quick Scan** is recommended.
- **Flash Scan:** Scans memory and autorun objects only.

After selecting the type of scan – and drives for a Full Scan – click the **Scan** button to initiate the scan. While the scan is running, the screen will show status of the scan in progress. A screenshot of this screen is shown below.



Scanner
Malwarebytes Anti-Malware is now scanning your system. Please wait until the scan is complete.

Scanning memory objects for infection.
Objects scanned: 1281
Objects detected: 0

Scan type: Quick scan
Time elapsed: 20 second(s)

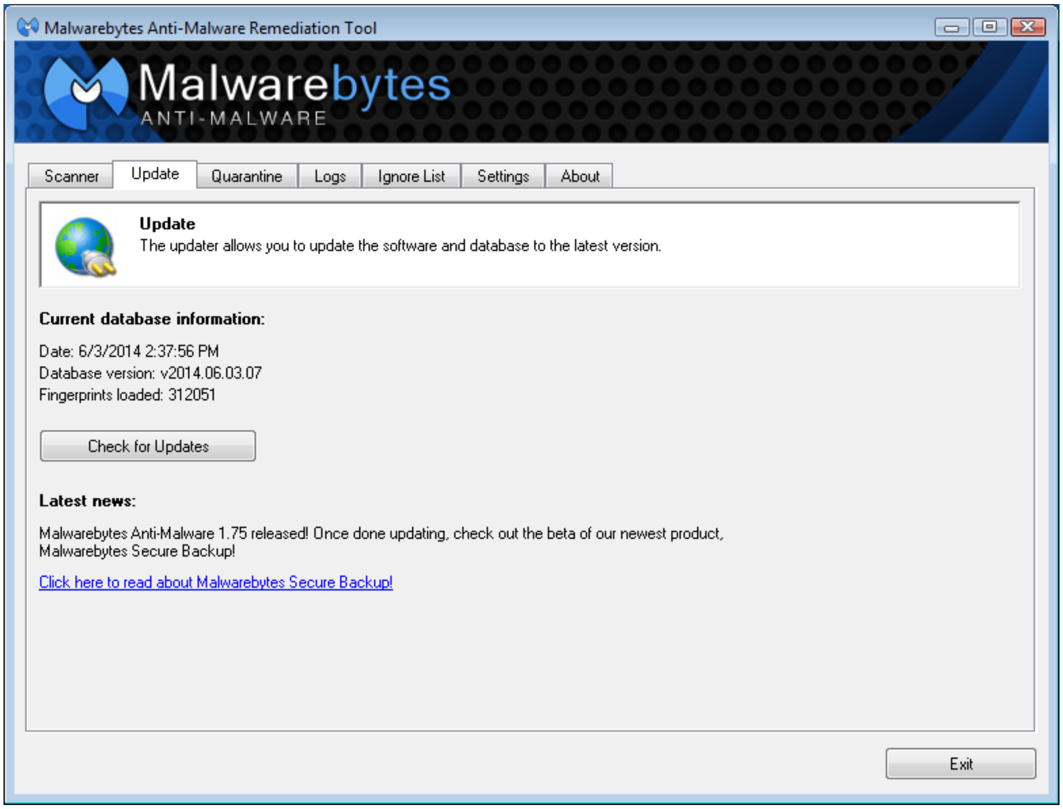
Currently scanning:
C:\WINDOWS\SYSTEM32\MSCOREE.DLL

The amount of time required to execute a scan varies widely, depending on the type of scan and the age of the endpoint. A *Flash Scan* is very fast, typically in the neighborhood of 1-2 minutes duration. A *Quick Scan* requires less than 10 minutes. A *Full Scan* may take more than an hour for an endpoint which has been in use for an extended period of time. As a general rule, endpoints which have been *well used* will also have hundreds of thousands of file which must be analyzed. This unavoidably takes time. A newer (or *less busy*) endpoint will require less time because there is less work to do.

Once the scan has completed, a status message will be presented in the middle of your screen. A log which details the scan will be displayed on your screen, and also saved to the *Logs* directory.

## 2.3 Update Tab

This tab provides information about the signature database which *Malwarebytes Anti-Malware Remediation Tool* uses to provide protection, as well as allowing the user to check for updates immediately. A screenshot of this tab is shown here.



**Update**
The updater allows you to update the software and database to the latest version.

**Current database information:**

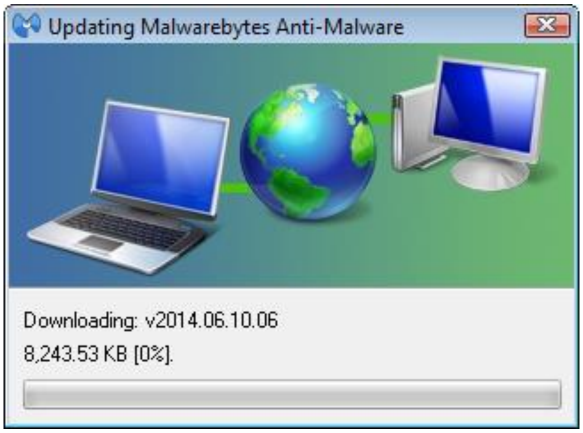
Date: 6/3/2014 2:37:56 PM
Database version: v2014.06.03.07
Fingerprints loaded: 312051

**Latest news:**

Malwarebytes Anti-Malware 1.75 released! Once done updating, check out the beta of our newest product, Malwarebytes Secure Backup!

Click here to read about Malwarebytes Secure Backup!

By clicking the *Check for Updates* button, *Malwarebytes Anti-Malware Remediation Tool* will contact a Malwarebytes internet server and check for available database updates. If an update is available, it will be downloaded and merged into the program's signature database.

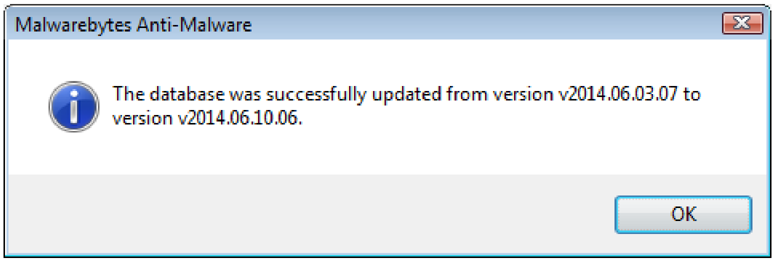


Downloading: v2014.06.10.06
8,243.53 KB [0%].

Updates are typically available 6-15 times daily. Because *Malwarebytes Anti-Malware Remediation Tool* is a portable product, updates cannot be received on a scheduled basis. This results in larger updates, though the size of the database as a whole is less than ten megabytes.

**HINT:** An IT Administrator could maintain a copy of *Malwarebytes Anti-Malware Remediation Tool* in its extracted form, so that database updates could be downloaded and integrated into the file set prior to re-archiving and deployment.

Following a successful update, a user notification will be provided in a dialog box similar to the one shown here.



Malwarebytes Anti-Malware

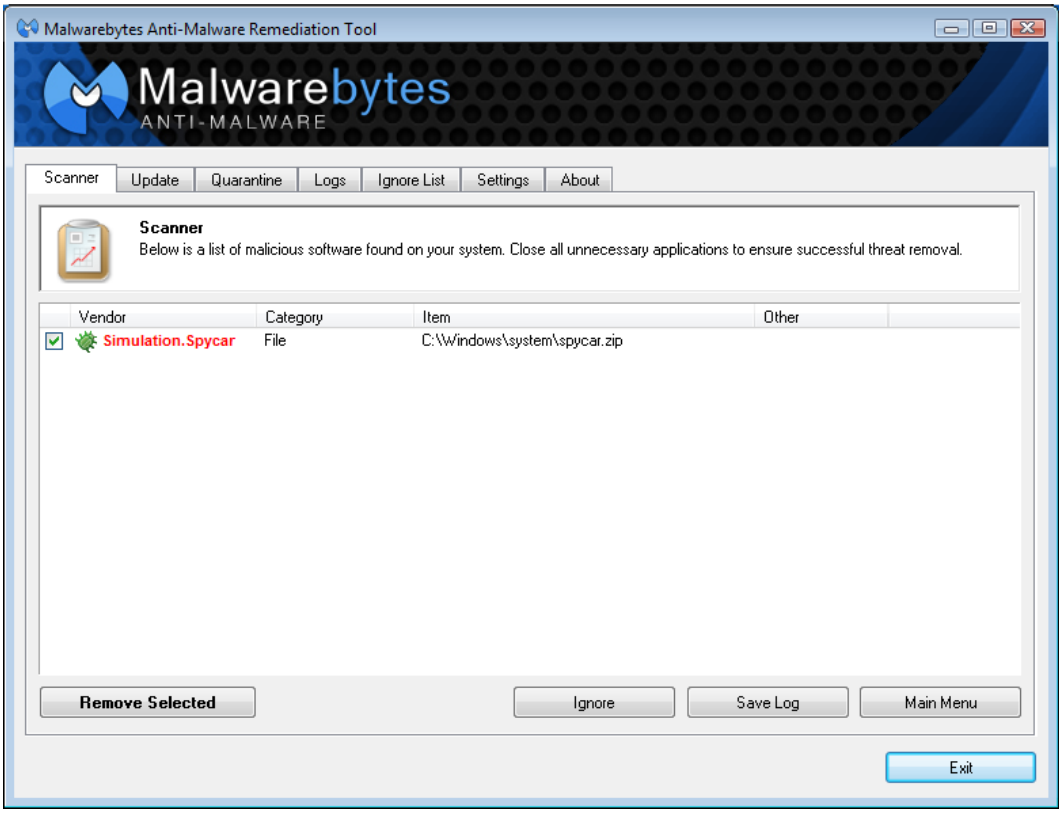
The database was successfully updated from version v2014.06.03.07 to version v2014.06.10.06.

Please note that database updates are shown using the format v*yyyy.mm.dd.##*, which specifies the year, month, day, and update number released on the day listed. While the exact time of the update is not shown as part of the filename, dates shown are referenced to Greenwich Mean Time. New York's time zone is GMT-5 (summer GMT-4). San Francisco's time zone is GMT-8 (summer GMT-7). Using those two cities as a reference point for this example, it is possible that updates issued in late afternoon or evening (San Francisco time), or late evening (New York time) would show a date stamp that appears to be in the future. This piece of knowledge may save some confusion.

Additional Update functionality is also available via the command line. This will be discussed later in this guide.

## 2.4 Quarantine Tab

This tab provides a record of all potential threats which have been detected and prevented from causing any damage. A screenshot is shown below.



**Scanner**

Below is a list of malicious software found on your system. Close all unnecessary applications to ensure successful threat removal.

| Vendor | Category | Item | Other |
|---|---|---|---|
| ☑ Simulation.Spycar | File | C:\Windows\system\spycar.zip | |

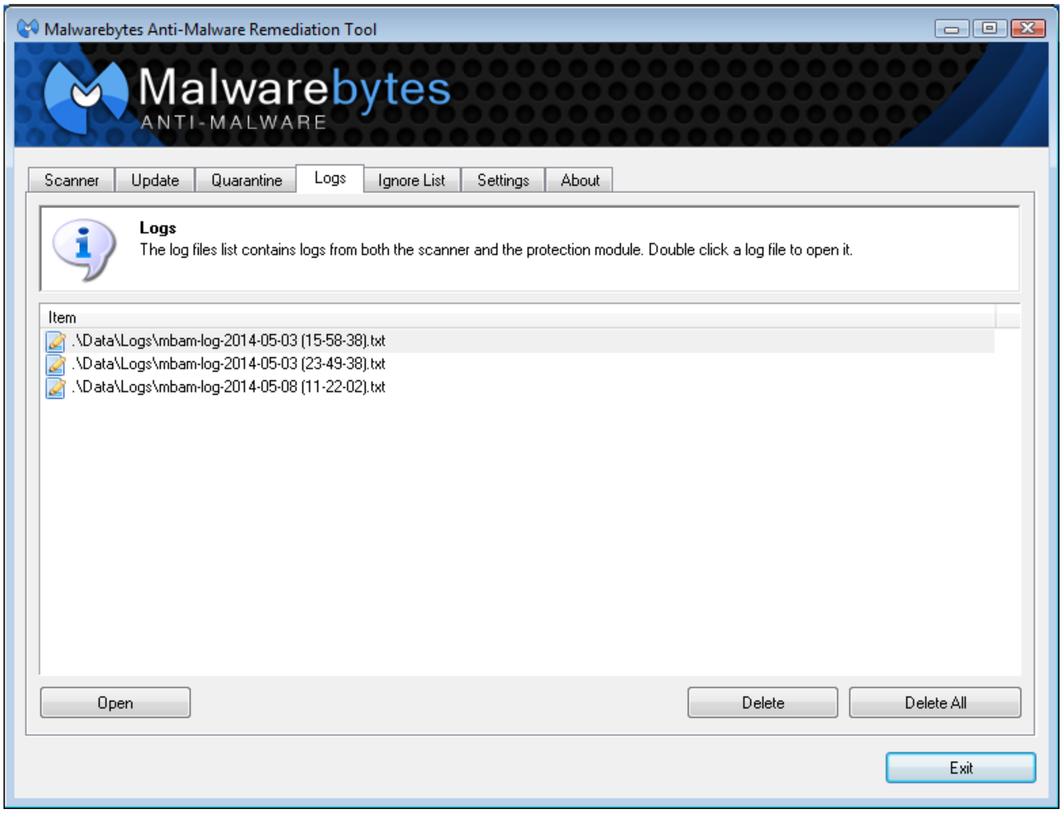
In this screenshot, one file has been detected and isolated so that it cannot cause damage. As part of pertinent information about the file, its location – prior to being quarantined – is shown. This is important to note, because the file may be legitimate. If the user is unsure about the file's legitimacy, it is up to them to research via the internet or to visit the Malwarebytes public forums in an attempt to learn more about the file before making a final decision. Below the file list, four buttons are available to allow the user to act upon the potential threats. These are:

- **Delete:** Delete a file which has been selected by highlighting it.
- **Delete All:** Delete all files shown on the list
- **Restore:** Restore a file which has been selected by highlighting it.
- **Restore All:** Restore all files shown on the list

## 2.5 Logs Tab

*Malwarebytes Anti-Malware Remediation Tool* produces a log file as part of each scan which it executes. This tab provides an itemization of those logs, and allows access to them as well. Each log file contains program configuration and scan results. The file's name is based on the endpoint's internal clock, and shows the date and time that the scan was initiated. In the case of a full system scan, that could be an hour or more prior to the scan's completion time. Knowing this may help avoid some confusion. The location of the log is shown along with the filename.

A screenshot of the **Logs** screen is shown here.



**Logs**

The log files list contains logs from both the scanner and the protection module. Double click a log file to open it.

Item
.\Data\Logs\mbam-log-2014-05-03 (15-58-38).txt
.\Data\Logs\mbam-log-2014-05-03 (23-49-38).txt
.\Data\Logs\mbam-log-2014-05-08 (11-22-02).txt

You may open any log by highlighting it and clicking the **Open** button. You may delete any log by highlighting it and clicking the **Delete** button. You may delete all logs at once by clicking the **Delete All** button.

## 2.6 Ignore List Tab

This tab contains an itemization of files which are ignored by the scanner. You may add files to this list via a Windows Explorer-like window displayed when you click the **Add** button. You may delete individual files by highlighting the file and clicking the **Delete** button, and you may delete all files from the list by clicking the **Delete All** button.

Files may also be added to this list if a threat is detected, and you elect to quarantine the detected file.

**NOTE:** If a password has been defined (in **Settings**), it will be required to access this tab. See Section 2.7 for further details.

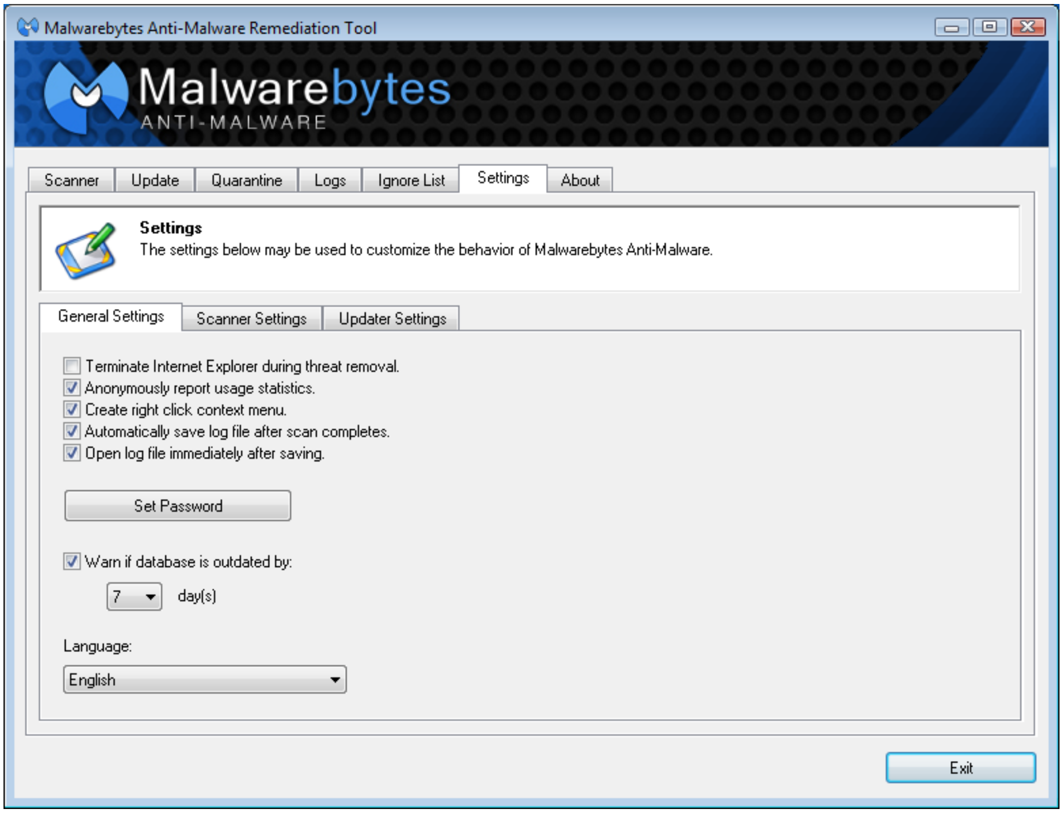
## 2.7 Settings Tab

This tab provides a majority of the configuration settings for *Malwarebytes Anti-Malware Remediation Tool*. In order to provide an uncluttered interface, this tab is subdivided into three tabs. We will look at each of those tabs in detail here.

**NOTE:** If a password has been set, it will be required to access this tab.

### 2.7.1 General Settings

This tab contains several settings which control basic behavior of *Malwarebytes Anti-Malware Remediation Tool*. A screenshot of the *General Settings* tab is shown below.



**Settings**
The settings below may be used to customize the behavior of Malwarebytes Anti-Malware.

☐ Terminate Internet Explorer during threat removal.
☑ Anonymously report usage statistics.
☑ Create right click context menu.
☑ Automatically save log file after scan completes.
☑ Open log file immediately after saving.

☑ Warn if database is outdated by:
7 day(s)

Language:
English

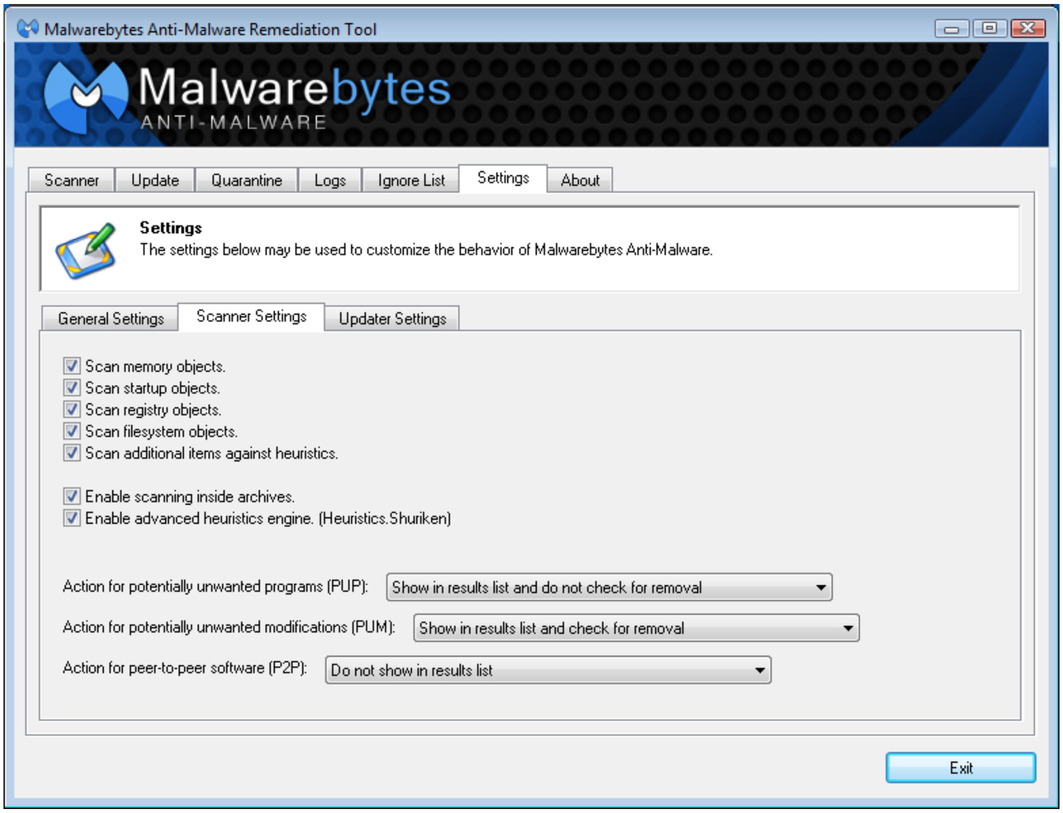
Individual settings which may be configured here are:

- **Terminate Internet Explorer during threat removal:** Enabling this option allows *Malwarebytes Anti-Malware Remediation Tool* to terminate Internet Explorer browsing sessions automatically before removing threats detected in the Temporary Internet Files folder. If this setting is not enabled, a reboot may be required to complete the threat removal process for these types of infections. **Please note** that when this setting is enabled, any work that is currently in process may be lost if a reboot is required.

- **Anonymously report usage statistics:** This option automatically collects statistical information on malware threats detected on your system, and reports that information to our Threat Research Center. No personally identifiable or personal information is collected.
- **Create right click context menu:** This option is disabled in *Malwarebytes Anti-Malware Remediation Tool*.
- **Automatically save log file after scan completes:** Create a log file each time a scan is performed.
- **Open log file immediately after saving:** Automatically open the log file created by the scan once the scan has completed.
- **Set Password:** Set a password. Any characters except for quotes (") are allowed to be used. To reset/remove the password, click the *Set Password* button, enter the current password, and then leave both fields blank and click **Submit**. The password restricts access to the *Ignore List* and *Settings* tabs.
- **Warn if database is outdated by <x> days:** If a database update has not occurred within <x> days, this option enables display of a pop-up notification to warn the user that database signatures are outdated.
- **Language:** This option is disabled in *Malwarebytes Anti-Malware Remediation Tool*.

### 2.7.2 Scanner Settings

This tab controls settings which are specific to scanning functionality within the program. A screenshot is shown below.



**Settings**
The settings below may be used to customize the behavior of Malwarebytes Anti-Malware.

☑ Scan memory objects.
☑ Scan startup objects.
☑ Scan registry objects.
☑ Scan filesystem objects.
☑ Scan additional items against heuristics.

☑ Enable scanning inside archives.
☑ Enable advanced heuristics engine. (Heuristics.Shuriken)

Action for potentially unwanted programs (PUP): Show in results list and do not check for removal

Action for potentially unwanted modifications (PUM): Show in results list and check for removal

Action for peer-to-peer software (P2P): Do not show in results list

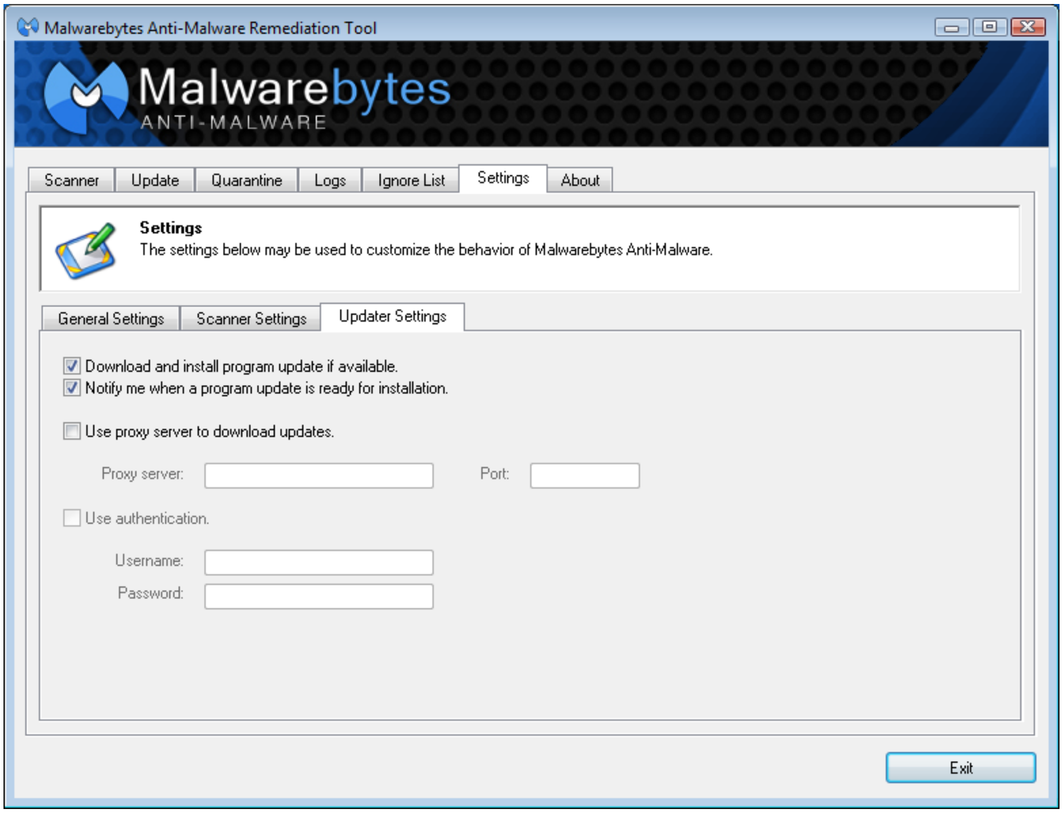
Individual settings which may be configured here are:

- **Scan Memory Objects:** Scans all processes running in memory when a scan is performed to check for actively running infections.
- **Scan StartUp Objects:** Scans known startup locations which threats might use to start themselves when the computer boots.
- **Scan Registry Objects:** Scans the Windows registry to check for installed threats and malicious alterations of certain Windows settings.

- **Scan Filesystem Objects:** Scans files and folders on the system to check for infected files. The number of files and folders scanned and their location varies depending on the type of scan.
- **Scan Additional Items Against Heuristics:** Performs a check of key files, folders and registry locations against our very powerful heuristics database to look for infections not found by other parts of the scan.
- **Enable Scanning inside Archives:** Includes checking archive files (ZIP, RAR etc.) in the locations scanned.
- **Enable Advanced Heuristics Engine (Heuristics Shuriken):** Enables our latest heuristics detection engine to perform a more advanced analysis of the system for new threats not in our detection database, possibly finding threats the other parts of the scan cannot yet find.
- **Action for Potentially Unwanted Programs (PUP):** Detects known, non-malicious software which may causes undesirable performance or issues for the computer.
- **Action for Potentially Unwanted Modifications (PUM):** Identifies system setting modifications which may have an adverse effect or direct impact on available functionality or system resources.
- **Action for Peer-To-Peer Software (P2P):** Detects file sharing software installed on the system. Available actions and definition for the above 3 settings:
  - **Do not show in results list:** Items of this type will not be detected or shown in the scanned results list.
  - **Show in results list and check for removal:** Items of this type will be detected, shown in the results list and marked for removal.
  - **Show in results list and do not check for removal:** The detected item is shown in the scan results list but will not be selected for removal. Each item must be checked manually for removal.

### 2.7.3 Updater Settings

This tab provides settings pertaining to program updates and communication settings required for **<u>all</u>** updates. A screenshot is shown below.



**Settings**
The settings below may be used to customize the behavior of Malwarebytes Anti-Malware.

☑ Download and install program update if available.
☑ Notify me when a program update is ready for installation.

☐ Use proxy server to download updates.

Proxy server: ______ Port: ______

☐ Use authentication.

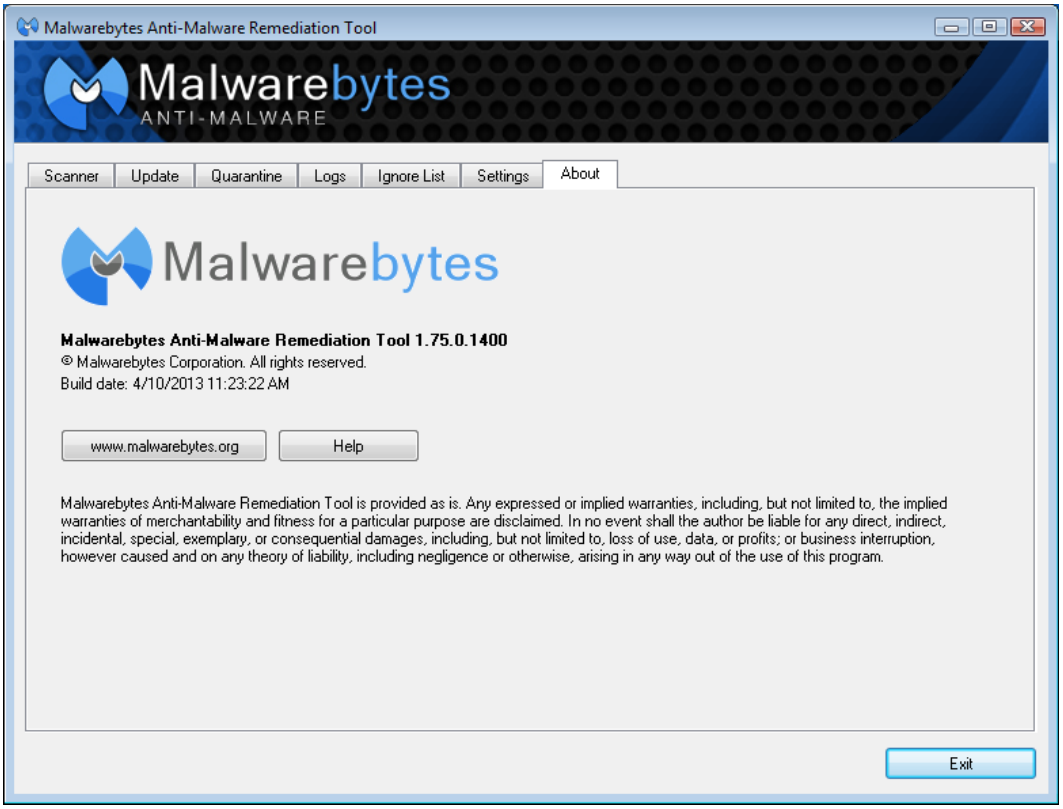
Username: ______
Password: ______

Individual settings which may be configured here are:

- **Download and install program update if available:** When checked, new programs versions (if available) will be downloaded automatically whenever the program checks for database updates.
- **Notify me when a program update is ready for installation:** If a program update has been downloaded and this checkbox is enabled, the system tray icon will display a tooltip balloon to let the user know that a new version of *Malwarebytes Anti-Malware Remediation Tool* has been downloaded and is ready to be installed.
- **Use proxy server to download updates:** When checked, the IP address (or Fully-Qualified Domain Name) and port number of a proxy server must be specified. If a proxy server is needed for communication to the public internet, this setting *is mandatory* to receive program updates and database updates.
- **Use authentication:** If a proxy server is used and requires user authentication, this box should be checked and a valid username/password combination should be supplied. This is used only for proxy server communications, and nowhere else in the program.

## 2.8 About Tab

This tab is primarily informational in nature. It is shown below.



**Malwarebytes Anti-Malware Remediation Tool 1.75.0.1400**
© Malwarebytes Corporation. All rights reserved.
Build date: 4/10/2013 11:23:22 AM

Malwarebytes Anti-Malware Remediation Tool is provided as is. Any expressed or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the author be liable for any direct, indirect, incidental, special, exemplary, or consequential damages, including, but not limited to, loss of use, data, or profits; or business interruption, however caused and on any theory of liability, including negligence or otherwise, arising in any way out of the use of this program.

The version and build number of the program are provided here. This information would be requested from you if you contacted Malwarebytes Technical Support for assistance. There are also buttons which (when clicked) link you to the Malwarebytes web site, and to an abbreviated form of this guide.

# 3.0 Command Line Parameters

*Malwarebytes Anti-Malware Remediation Tool* supports a variety of command line parameters, which can be used from a command prompt, batch file or script. When used from a script, additional commands may be required to support the scripting model being used.

## 3.1 Conventions

The command line structure uses parameters and modifiers. Parameters are specified with a forward slash ("/") and modifiers are called with a hyphen ("-"). They must be separated by spaces. Multiple modifiers may be combined with a parameter. In addition, the following conventions are used:

- Required specifications are encased by angle brackets
  Example: **mbam <parameter_1>**
- Optional specifications are encased by square brackets
  Example: **mbam <parameter_1> [parameter_2]**
- Repeated items are shown by a grouping of dots
  Example: **mbam <parameter _1> [parameter_2] … [parameter_n]**
- Choice of specifications are separated by vertical bars
  Example: **mbam <0|1|2|3>**

## 3.2 Command Line Reference

Commands listed here are listed individually, though multiple parameters may be included in the same command. These are primarily used by a system administrator via script, batch file, GPO update, or remote desktop. The admin may configure *Malwarebytes Anti-Malware Remediation Tool* to operate as a remote task, invisible to the endpoint user. When this is the case, command line tools offer the only method of modifying program configuration on the endpoint.

### 3.2.1 Suppress Error Reporting

**Usage:**

**mbam /errorsilent**

**Purpose:**

Suppresses all critical errors during operation and write the last error to <root-drive>\mbam-error.txt, where <root-drive> is the drive where Windows is installed (System Drive).

**Parameters:**

none

### 3.2.2 Update

**Usage:**

**mbam /update [-silent]**

**Purpose:**

Request an update for the *Malwarebytes Anti-Malware* signature database, and check for program updates. If updates are found, they will be integrated automatically.

**Parameters:**

| | |
|---|---|
| **-silent** | Perform the update check in the background (invisible to the user) |

**Examples:**

- **mbam /update** checks for program/database updates
- **mbam /update –silent** checks for program/database updates in the background

### 3.2.3 Proxy Communications

**Usage:**

**mbam /proxy [server] [port] [username] [password]**

**Purpose:**

This command defines proxy settings which may be required to receive database updates. Leave blank to remove previously-defined proxy settings.

**Parameters:**

**server** Enter an IP address or server name if required to access the internet

**port** Enter communication port number defined for proxy communications

**username** Enter a username if required

**password** Enter a password if authentication is required

**Examples:**

- **mbam /proxy** will remove defined proxy settings.
- **mbam /proxy proxy.com 80** will use proxy.com on port 80 with no credentials.
- **mbam /proxy proxy.com 80 admin password** will use proxy.com with the specified credentials.

### 3.2.4 Scan

**Usage:**

**mbam /scan [-quick|-full|-flash] [-silent] [-remove] [-terminate] [-reboot] [-log]**

**Purpose:**

Perform a scan according to specifications provided.

**Parameters:**

**-quick** Perform a quick scan.

**-full** Perform a full scan on all non-removable drives.

**-flash** Perform a flash scan (memory and heuristics only).

**-terminate** Closes the program after a scan completes if no threats were found (cannot be used with **-silent**). If an item is detected, the program remains open so that the user can decide whether or not to remove the detected threat(s).

**-log** Overrides the **Save Log** checkmark on the settings tab. If the **Automatically save log after scan completes** option is unchecked, a log file will still be saved when the **-log** parameter is used.

**-silent** Hides the GUI while scanning (does not need to be used with **-terminate**).

**-reboot** Reboots the computer if necessary, only valid if **-remove** is used.

**-remove** Automatically removes threats and saves a log file. GUI stays open unless **-silent** is specified.

**Examples:**

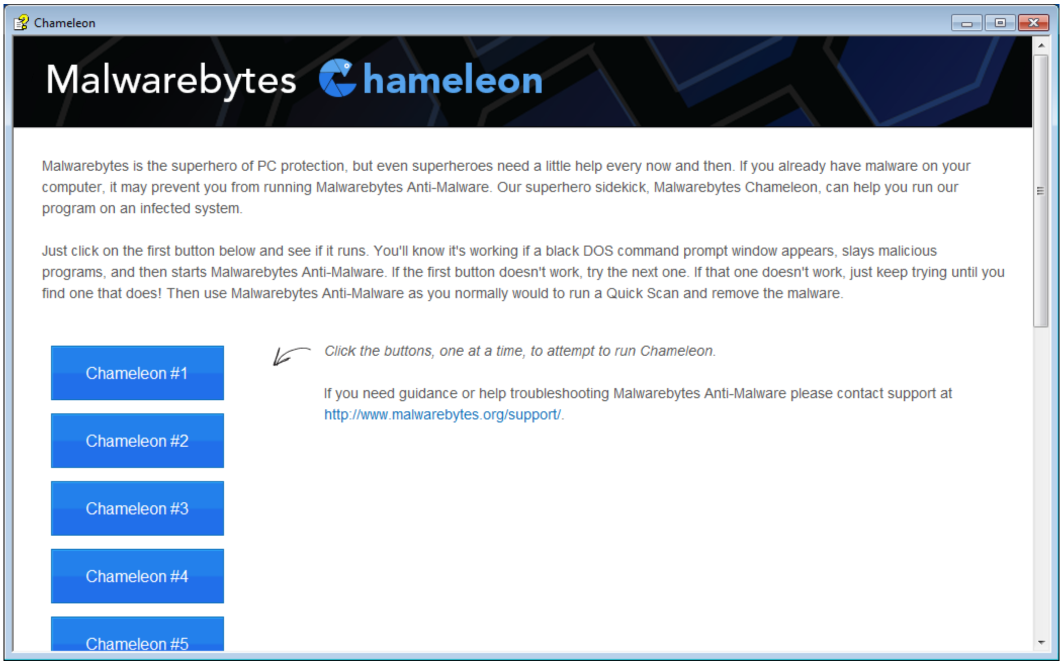
- **mbam /scan** will run a default scan.
- **mbam /scan -full** will run a full scan.
- **mbam /scan -flash -terminate** will run a flash scan and terminate if no objects are detected.
- **mbam /scan -quick -log -silent -remove -reboot** runs a silent quick scan, saves logs, automatically removes threats, and reboots if necessary.

**Limitations:**

- **-terminate** cannot be used with **-silent** since the program will automatically terminate when **-silent** is used.
- **-reboot** is only valid if used with **-remove**.

# 4.0 Malwarebytes Chameleon

*Malwarebytes Chameleon* is a set of new technologies designed to allow *Malwarebytes Anti-Malware* to execute on a computer when it has been prevented from doing so by specific malware infections. There are several methods available to launch Chameleon, all of which are detailed in the following steps. The screenshot below shows the Chameleon program screen once the program has been launched. Please note that this screen has been resized so that all text can be shown.



Malwarebytes is the superhero of PC protection, but even superheroes need a little help every now and then. If you already have malware on your computer, it may prevent you from running Malwarebytes Anti-Malware. Our superhero sidekick, Malwarebytes Chameleon, can help you run our program on an infected system.

Just click on the first button below and see if it runs. You'll know it's working if a black DOS command prompt window appears, slays malicious programs, and then starts Malwarebytes Anti-Malware. If the first button doesn't work, try the next one. If that one doesn't work, just keep trying until you find one that does! Then use Malwarebytes Anti-Malware as you normally would to run a Quick Scan and remove the malware.

*Click the buttons, one at a time, to attempt to run Chameleon.*

If you need guidance or help troubleshooting Malwarebytes Anti-Malware please contact support at http://www.malwarebytes.org/support/.

The primary methods of accessing and using Chameleon are shown below.

## 4.1 Using the Chameleon.chm Help File via Explorer

1. Go to the directory where you installed *Malwarebytes Anti-Malware Remediation Tool*, navigate to the **Chameleon** subdirectory, and double-click on the **chameleon.chm** help file.
2. Once the “Help” file opens, click each **Chameleon #** button until you see a black DOS/command prompt window that remains open and says MBAM-chameleon ver. # at the top. If your host operating system is Windows Vista, Windows 7 or Windows 8, you may see a User Account Control prompt. If so, click **Yes.**
3. Press any key to continue.
4. *Malwarebytes Chameleon* will then update *Malwarebytes Anti-Malware*. Please ensure that you are connected to the internet if possible. Once the update completes and it says your database has been updated, click **OK.**
5. *Malwarebytes Chameleon* will then terminate threats running in memory. Please be patient…this may take a while. Upon completion, *Malwarebytes Anti-Malware* will open automatically and perform a Quick Scan.
6. Once the scan is complete, click on **Show Results.** You may remove any threats which have been found by clicking **Remove Selected.**
7. If prompted to restart the computer to complete the removal process, click **Yes.**
8. After the computer restarts, open *Malwarebytes Anti-Malware* and perform one last Quick Scan to verify that no threats remain.

## 4.2 Using the Chameleon.chm Help File via Task Manager

1. Press **Ctrl**+**Shift**+**Esc** on the keyboard.
2. Once **Task Manager** opens, click on **File** at the top and choose **New Task (Run...)**.
3. Click the **Browse...** button.
4. Navigate to the **Chameleon** subdirectory underneath *Malwarebytes Anti-Malware Remediation Tool*.
5. Click on the drop-down menu that says **Programs** and choose **All Files**.
6. Double-click on the **Chameleon.chm** help file.
7. Once the "Help" file opens, click each **Chameleon #** button until you see a black DOS/command prompt window that remains open and says MBAM-chameleon ver. # at the top.
8. Press any key to continue.
9. *Malwarebytes Chameleon* will then update *Malwarebytes Anti-Malware*. Please ensure that you are connected to the internet if possible. Once the update completes and it says your database has been updated, click **OK**.
10. *Malwarebytes Chameleon* will then terminate threats running in memory. Please be patient…this may take a while. Upon completion, *Malwarebytes Anti-Malware* will open automatically and perform a Quick Scan.
11. Once the scan is complete, click on **Show Results**. You may remove any threats which have been found by clicking **Remove Selected**.
12. If prompted to restart the computer to complete the removal process, click **Yes**.
13. After the computer restarts, open *Malwarebytes Anti-Malware* and perform one last Quick Scan to verify that no threats remain.

## 4.3 Using the Chameleon.chm Help File via Internet Browser

1. Open the internet browser (for example, **Internet Explorer**, **Firefox** or **Google Chrome**).
2. Press the **Alt** key on the keyboard.
3. In the menu that appears at the top, click on **File** and choose **Open** or **Open File**.
4. In the browse window that opens, navigate to the **Chameleon** subdirectory underneath *Malwarebytes Anti-Malware Remediation Tool*.
5. Double-click on the **Chameleon.chm** help file. If you do not see it, click on the drop-down menu that says **Web Documents** and choose **All Files**.
6. Once the "Help" file opens, click each **Chameleon #** button until you see a black DOS/command prompt window that remains open and says MBAM-chameleon ver. # at the top. If your host operating system is Windows Vista, Windows 7 or Windows 8, you may see a User Account Control prompt. If so, click **Yes**.
7. Press any key to continue.
8. *Malwarebytes Chameleon* will then update *Malwarebytes Anti-Malware*. Please ensure that you are connected to the internet if possible. Once the update completes and it says your database has been updated, click **OK**.
9. *Malwarebytes Chameleon* will then terminate threats running in memory. Please be patient…this may take a while. Upon completion, *Malwarebytes Anti-Malware* will open automatically and perform a Quick Scan.
10. Once the scan is complete, click on **Show Results.** You may remove any threats which have been found by clicking **Remove Selected**.
11. If prompted to restart the computer to complete the removal process, click **Yes**.
12. After the computer restarts, open *Malwarebytes Anti-Malware* and perform one last Quick Scan to verify that no threats remain.

## 4.4 Chameleon.chm Will Not Open Due to Infection

1. Navigate to the **Chameleon** subdirectory underneath *Malwarebytes Anti-Malware Remediation Tool*.
2. Next, double-click on each file one by one until you find one that works, which will be indicated by a black DOS/command prompt window. If your host operating system is Windows Vista, Windows 7 or Windows 8, you may see a User Account Control prompt when attempting to open the files. If so, click **Yes**

**Warning:** Do not attempt to open file **mbam-killer.exe.** This file serves a different purpose.

3. Press any key to continue.
4. *Malwarebytes Chameleon* will then update *Malwarebytes Anti-Malware*. Please ensure that you are connected to the internet if possible. Once the update completes and it says your database has been updated, click **OK**.
5. *Malwarebytes Chameleon* will then terminate threats running in memory. Please be patient…this may take a while. Upon completion, *Malwarebytes Anti-Malware* will open automatically and perform a Quick Scan.
6. Once the scan is complete, click on **Show Results**. You may remove any threats which have been found by clicking **Remove Selected**.
7. If prompted to restart the computer to complete the removal process, click **Yes**.
8. After the computer restarts, open *Malwarebytes Anti-Malware* and perform one last Quick Scan to verify that no threats remain.

## 4.5 Other Methods

You may also mix the techniques described above. For example, if the CHM help file will not open via Task Manager or an internet browser, you can use that same method to try and run the Chameleon executables one by one. You can also try booting the endpoint into Safe Mode with Networking (so that you have internet access for downloading updates).

## 5.0 Open Source Licenses

Malwarebytes uses a variety of Open Source components. Each of these components' licenses are below.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/). This product includes software licensed under the Apache 2.0 license. This product includes software licensed under the MIT license. This product includes software developed by vbAccelerator (http://vbaccelerator.com/).

## 5.1 OpenSSL License

```
  OpenSSL License
  ---------------

/* ====================================================================
 * Copyright (c) 1998-2011 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */

 Original SSLeay License
 -----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscape’s SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the routines from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *    the apps directory (application code) you must include an acknowledgement:
 *    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed.  i.e. this code cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */
```

## 5.2 MIT License

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## 5.3 Apache License

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor

has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

## 5.4 vbAccelerator License

vbAccelerator Software License
Version 1.0

Copyright (c) 2002 vbAccelerator.com

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by vbAccelerator (http://vbaccelerator.com/)." Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

The names "vbAccelerator" and "vbAccelerator.com" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact vbAccelerator through steve@vbaccelerator.com. Products derived from this software may not be called "vbAccelerator", nor may "vbAccelerator" appear in their name, without prior written permission of vbAccelerator.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL VBACCELERATOR OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.