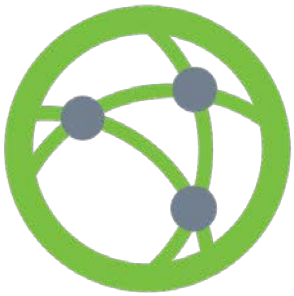


Malwarebytes
ENDPOINT
SECURITY

Malwarebytes Anti-Malware
Unmanaged Client Administrator Guide

Version 1.80

11 October 2016

Malwarebytes

Notices

Third Party Project Usage

Malwarebytes software is made possible thanks in part to many open source and third party projects. A requirement of many of these projects is that credit is given where credit is due. The *Malwarebytes Third Party License Supplement* is a downloadable reference which specifies each of these projects, and where they are used. It can be downloaded from:

https://www.malwarebytes.com/pdf/guides/ThirdPartyLicenseSupplement.pdf

Sample Code in Documentation

The sample code described herein is provided on an "as is" basis, without warranty of any kind, to the fullest extent permitted by law. Malwarebytes does not warrant or guarantee the individual success developers may have in implementing the sample code on their development platforms. You are solely responsible for testing and maintaining all scripts.

Malwarebytes does not warrant, guarantee or make any representations regarding the use, results of use, accuracy, timeliness or completeness of any data or information relating to the sample code. Malwarebytes disclaims all warranties, express or implied, and in particular, disclaims all warranties of merchantability, fitness for a particular purpose, and warranties related to the code, or any service or software related there to.

Table of Contents

Table of Contents (continued)

System Requirements

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

- **Operating System:**
  - Windows 10 (32/64-bit)
  - 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 3 or later, 32-bit only)
  - Windows Server 2012/2012 R2 (32/64-bit)
  - Windows Server 2008/2008 R2 (32/64-bit)
  - Windows Server 2003 (32-bit only)
  - Windows Small Business Server 2011

  Please note that Windows server using the Server Core installation process is specifically excluded.

- **CPU:** 800 MHz or faster
- **RAM:** 2048 MB (server OS), 1024 MB (client OS except Windows XP), 256 MB (Windows XP)
- **Free Disk Space:** 25 MB
- **Screen Resolution:** 800x600 or higher
- **Active Internet Connection**

Introduction

Malwarebytes Anti-Malware is a next-generation anti-malware program that can quickly detect, destroy and block malicious software. *Malwarebytes Anti-Malware* can detect and remove malware that even many of the most well-known anti-virus and anti-malware applications on the market today cannot.

Malwarebytes Anti-Malware monitors every process and stops malicious processes before they even start. The scanner and real-time Protection Module both use our advanced heuristic scanning technology to keep your system safe and secure against even the latest malware threats.

In addition, *Malwarebytes Anti-Malware* provides an extensive API which allows a system administrator to install, configure and manage endpoints using a powerful command line interface.

What's New

The following changes have been made in this version of *Malwarebytes Anti-Malware*.

Improvements:

- Added substantial improvements to core detection and removal technology
- Enhanced safeguards to prevent false positives on legitimate files
- Added support for Windows 10, Windows Server 2003 (32-bit), Windows Server 2008 and Windows Server 2012 operating systems
- Added capability to download incremental updates directly from the Internet
- Modified incremental database update process to allow 50 incremental updates before requiring a full database update

Issues Fixed:

- Fixed issue which caused BSOD when scanning a drive encrypted with BitLocker
- Resolved various issues that could result in crashes or system hangs

Key Features

Malwarebytes Anti-Malware is an anti-malware application with the following features:

- Real-time protection works together with leading anti-virus utilities to make your computer more secure.
- Real-time Protection detects and blocks threats whenever they try to execute.
- Malicious website blocking prevents access to malicious and infected websites.
- Scheduled updates to keep protection up-to-date automatically.
- Scheduled scans so you can set it and forget it, knowing that your system will get checked as regularly as you desire.
- Lightning fast Flash Scans to check for immediately active threats on your system.
- Password protect your settings to prevent unauthorized changes.
- Light speed quick scanning.
- Ability to perform full scans for all drives.
- Database updates released daily to protect against the newest malware in-the-wild.
- Intelligent heuristics detect even the most persistent malware while remaining light on system resources.
- Quarantine to hold threats and restore them at your convenience.
- Ignore List for both the scanner and Protection Module.
- A small list of extra utilities to help remove malware manually.
- Dynamic Malwarebytes Chameleon technologies to get *Malwarebytes Anti-Malware* running when blocked by infection.
- Multi-lingual support.
- Context menu integration to scan files on demand.

Plus many more!

Installation

Malwarebytes Anti-Malware is available to business customers via download from the Malwarebytes website. Once downloaded, there are two methods by which *Malwarebytes Anti-Malware* may be installed. The first method is by launching the setup file in the graphical user interface (GUI). Second is by using the command line interface. Both are discussed below.

GUI-based Installation

Locate the icon/file for the *Malwarebytes Anti-Malware*, right click the file and select *Run as Administrator*. **It is mandatory that administrator privileges be used for this task.** If you are installing *Malwarebytes Anti-Malware* on a Windows version newer than Windows XP, a Windows dialog box will be presented in the middle of your screen, labeled **User Account Control**. Verify that the publisher is listed as Malwarebytes Corporation and click **Yes**. This is a Windows security feature that originated with Windows Vista, to assure that an application's capabilities are limited unless and until you authorize higher capabilities. Once approved, installation will begin. The installation program will display several screens which guide you through the installation, and allow 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:

- **Select Setup Language:** You may select from a number of languages to be used during the installation. The language chosen for installation will also be used for program operation.
- **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-Malware* will be stored here.
- **Additional Tasks:** You may also create a desktop icon here if you choose.
- **Ready to Install:** A final confirmation is required from you to perform the installation.
- **Installation Complete:** You may now launch *Malwarebytes Anti-Malware* at this time!

At this point, program installation is complete. You will see the *Malwarebytes Anti-Malware* user interface as shown below. If you have already purchased a Malwarebytes license, you may wish to activate your copy of *Malwarebytes Anti-Malware* at this time. You can do that now (or at any time) by clicking the **Activate** link at the lower left of the Malwarebytes user interface.

It is important to note that *Malwarebytes Anti-Malware* is not yet fully functional. You may not launch real-time protection – perhaps our most important feature – until the product has been activated.

Installation via the Command Line Interface

As with the GUI-based installation, this installation method also requires Administrator privileges. When launching the Windows command line interface (*cmd.exe*), right-click the file and select *Run as Administrator*.

Antivirus and Firewall Exclusions

Before continuing with this installation, it's necessary to mention possible interactions between *Malwarebytes Anti-Malware* and existing anti-virus and/or other security software which may be installed. Some antivirus and firewall applications require that you define file and folder exclusions to prevent conflicts with the program, and we recommend that you exclude *Malwarebytes Anti-Malware* and your antivirus from one another.

Example exclusions on XP

- C:\Program Files\Malwarebytes' Anti-Malware\mbam.exe
- C:\Program Files\Malwarebytes' Anti-Malware\mbamapi.exe
- C:\Program Files\Malwarebytes' Anti-Malware\mbamgui.exe
- C:\Program Files\Malwarebytes' Anti-Malware\mbamservice.exe
- C:\Program Files\Malwarebytes' Anti-Malware\mbamscheduler.exe
- C:\Program Files\Malwarebytes' Anti-Malware\mbam.dll
- C:\Program Files\Malwarebytes' Anti-Malware\mbamcore.dll
- C:\Program Files\Malwarebytes' Anti-Malware\mbamext.dll
- C:\Program Files\Malwarebytes' Anti-Malware\mbamnet.dll
- C:\Documents and Settings\All Users\Application Data\Malwarebytes\Malwarebytes' Anti-Malware\rules.ref
- C:\Windows\System32\drivers\mbam.sys

Example exclusions on Windows Vista and Windows 7 x64

- C:\Program Files (x86)\Malwarebytes' Anti-Malware\mbam.exe
- C:\Program Files (x86)\Malwarebytes' Anti-Malware\mbamapi.exe
- C:\Program Files (x86)\Malwarebytes' Anti-Malware\mbamgui.exe
- C:\Program Files (x86)\Malwarebytes' Anti-Malware\mbamservice.exe
- C:\Program Files (x86)\Malwarebytes' Anti-Malware\mbamscheduler.exe
- C:\Program Files (x86)\Malwarebytes' Anti-Malware\mbam.dll
- C:\Program Files (x86)\Malwarebytes' Anti-Malware\mbamcore.dll
- C:\Program Files (x86)\Malwarebytes' Anti-Malware\mbamext.dll
- C:\Program Files (x86)\Malwarebytes' Anti-Malware\mbamnet.dll
- C:\ProgramData\Malwarebytes\Malwarebytes' Anti-Malware\rules.ref
- C:\Windows\System32\drivers\mbam.sys

Most antivirus products have multiple locations within their GUI to make these exclusions beyond just a resident shield/on-access type setting. Vendors use different terms such as Identity Protection, PUPS, HIPS, Suspicious Activity, etc. If possible, exclusions generally need to be added in these areas as well. Some security programs store checksums of the exclusions and a main program update may necessitate re-applying the exclusions. Allow the following files through the firewall for updates to occur:

- C:\Program Files\Malwarebytes' Anti-Malware\mbam.exe
- C:\Program Files\Malwarebytes' Anti-Malware\mbamgui.exe
- C:\Program Files\Malwarebytes' Anti-Malware\mbamscheduler.exe
- C:\Program Files\Malwarebytes' Anti-Malware\mbamservice.exe

Also, make sure these DNS addresses are not blocked:

- http://data-cdn.mbamupdates.com
- https://data.service.malwarebytes.com

If you are unable to properly setup exclusions, please contact Malwarebytes Customer Success for assistance.

Email Address: corporate-support@malwarebytes.com

Command Line Installer Switches

Command line installation tasks are performed using the Malwarebytes installer, *mbam-setup.exe*. This program may be stored on a shared network drive, or stored locally on a computer which will be the target of the installation process. The installer may be invoked using the following command:

mbam-setup <parameter_1> … [parameter_n]

Please note that this section is also included in Appendix A, the *Command Line Reference Guide*, so that the guide can be a single consolidated reference for all *Malwarebytes Anti-Malware* commands. One or more parameters may be specified as *part* of the command. Following is a list of all parameters which may be used.

/dir=<path> Specifies an alternate installation directory. If the directory does not exist, it will be created here. **Please note:** The default installation directory is:

32-bit OS: *C:\Program Files\Malwarebytes' Anti-Malware*
64-bit OS: *C:\Program Files (x86)\Malwarebytes' Anti-Malware*

/log Causes setup to create a log file in the user's temporary directory detailing file installation and [Run] actions taken during the installation process.

/log="filename" Causes setup to create a log file in the specified location instead of the user's temporary folder, detailing file installation and [Run] actions taken during the installation process. This should include complete path and file name. The folder must already exist.

/nocancel Prevents the user from cancelling during the installation process, by disabling the *Cancel* button and ignoring clicks on the close button. Useful along with **/silent** or **/verysilent**.

Example: *mbam-setup /silent /nocancel*

/noicons	Instructs setup not to place shortcuts in the Windows Start Menu. Can be combined with **/tasks=""**. Example: *mbam-setup /noicons /tasks=""*
/norestart	Instructs setup not to reboot even if necessary Example: *mbam-setup /verysilent /nocancel /suppressmsgboxes /norestart*
/silent	
/verysilent	Instructs Setup to be silent or very silent. When Setup is silent, the wizard and the background window are not displayed but the installation progress window is displayed. When setup is very silent, the installation progress window is not displayed.
/suppressmsgboxes	Instructs setup to suppress message boxes. Only has an affect when combined with **/silent** and **/verysilent**.
/tasks=""	Instructs Setup not to place icons on the Windows desktop

Sample Batch File Installer

Malwarebytes has provided this sample script to assist you with understanding how our command line installation tools may be integrated into an installer script. In this script, the ID is shown as two groups of the string "xxxx" and the Key as four groups of the string "yyyy". Please replace both of these with the ID/key that were provided to you at the time of purchase. **Please note** that Malwarebytes cannot take responsibility for scripts written by customers, and cannot provide advice with regard to scripting.

```
REM Assumes that Malwarebytes has not been installed before
@echo off
echo+
echo ** Running Malwarebytes Anti-Malware installation batch script **
%~d0
cd %~dp0
mbam-setup.exe /nocancel  /norestart /verysilent /suppressmsgboxes
IF DEFINED programfiles(x86) (cd "%programfiles(x86)%\Malwarebytes' Anti-Malware") ELSE (cd "%programfiles%\Malwarebytes' Anti-Malware")
START /WAIT mbamapi.exe /register xxxxx-xxxxx yyyy-yyyy-yyyy-yyyy
START /WAIT mbamapi.exe /set hidereg on
START /WAIT mbamapi.exe /update
START /WAIT mbamapi /protection –install
START /WAIT mbamapi /protection -start
```

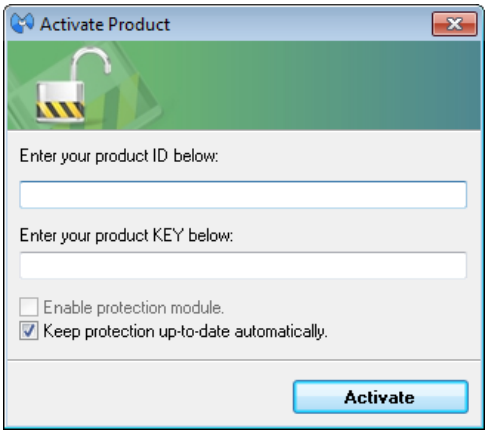
Sample VBScript Installer

Malwarebytes has provided this sample script to assist you with understanding how our command line installation tools may be integrated into an installer script. In this script, the ID is shown as two groups of the string "xxxx" and the Key as four groups of the string "yyyy". Please replace both of these with the ID/key that were provided to you at the time of purchase. **Please note** that Malwarebytes cannot take responsibility for scripts written by customers, and cannot provide advice with regard to scripting.

```
'Sample VBScript to install Malwarebytes - Only an example - testing and modification will be required.
On Error Resume Next
strComputer = "."
Set objShell = WScript.CreateObject("WScript.Shell")
Set objFilesys = CreateObject("Scripting.FileSystemObject")
If objFilesys.FileExists("C:\Program Files (x86)\Malwarebytes"&Chr(39)&" Anti-Malware\mbamapi.exe") Then
objShell.Run (""""C:\Program Files (x86)\Malwarebytes"&Chr(39)&" Anti-Malware\mbamapi.exe"" /register xxxxx-xxxxx yyyy-yyyy-yyyy-yyyy"),0,True
objShell.Run (""""C:\Program Files (x86)\Malwarebytes"&Chr(39)&" Anti-Malware\mbamapi.exe"" /update"),0,True
objShell.Run (""""C:\Program Files (x86)\Malwarebytes"&Chr(39)&" Anti-Malware\mbamgui.exe""  /install /silent"),0,True
Else
objShell.Run ("C:\DOWNLOAD\mbam-setup-1.80.2.1012.exe" & " /VERYSILENT /SUPRESSMSGBOXES /NOCANCEL"),0,True
objShell.Run (""""C:\Program Files (x86)\Malwarebytes"&Chr(39)&" Anti-Malware\mbamapi.exe"" /register xxxxx-xxxxx yyyy-yyyy-yyyy-yyyy"),0,True
objShell.Run (""""C:\Program Files (x86)\Malwarebytes"&Chr(39)&" Anti-Malware\mbamapi.exe"" /update"),0,True
objShell.Run (""""C:\Program Files (x86)\Malwarebytes"&Chr(39)&" Anti-Malware\mbamgui.exe""  /install /silent"),0,True
End If
Set objShell = Nothing
Set objFilesys = Nothing
```

Activation

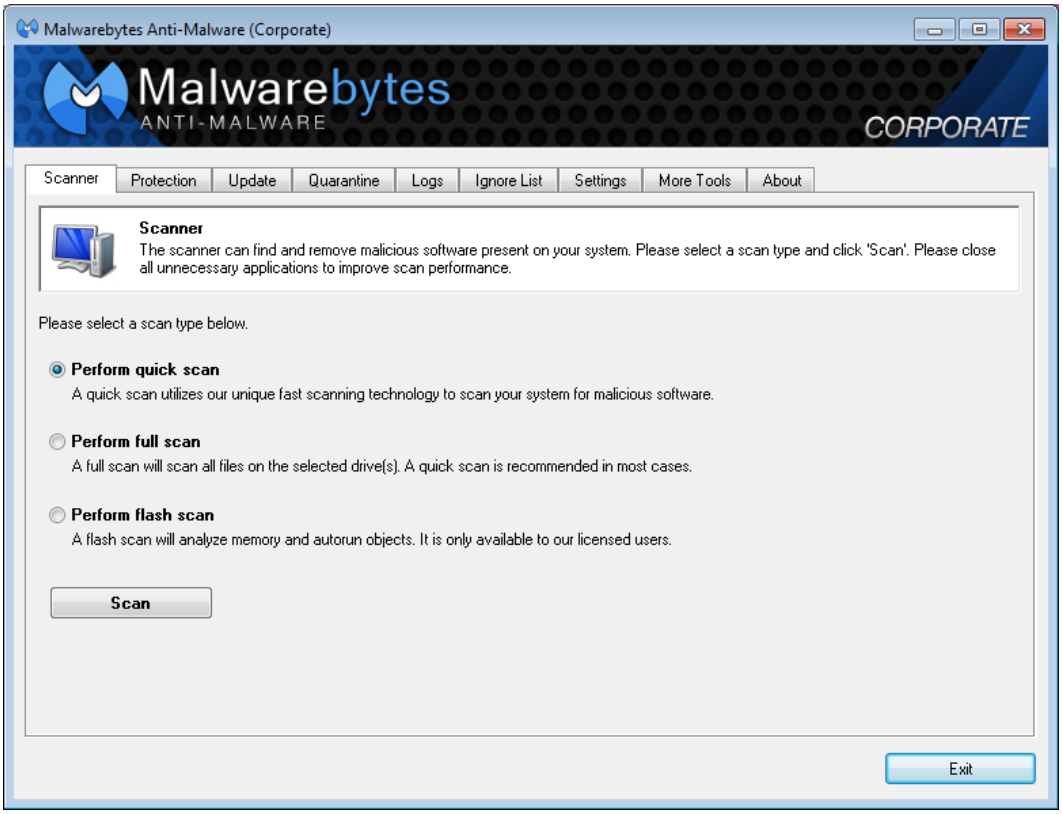
In the screenshot shown above, please note the **Buy Now** and **Activate** buttons in the lower left corner. When clicked, **Buy Now** takes the user to a screen which provides instructions on purchase of a *Malwarebytes Anti-Malware* license. If a license has been already purchased, clicking the **Activate** link shows the following screen...



Enter both the **ID** and **Key** in the spaces provided. You may also choose to enable the protection module, and to keep protection up-to-date automatically – Malwarebytes recommends both! Then, click the **Activate** button. The **Buy Now** and **Activate** buttons will both disappear once license information has been supplied and validated. A confirmation message will also be displayed at this time.

Screen Layout

The *Malwarebytes Anti-Malware* program interface is designed around a screen layout which is simplified and uncluttered. The screenshot shown below is what you will see each time that you launch the user interface.



Let's talk about the primary elements which make up our user interface.

Menu Bar

The Menu Bar consists of a row of tabs, each representing functional areas of the program. Each tab will be discussed here in detail, but in order to provide a basic introduction to the interface, here is a list of the tabs.

- **Scanner:** Selects a scan type and executes it.
- **Protection:** Configures and controls real-time protection.
- **Update:** Provides status of signature database, and enables on-demand update.
- **Quarantine:** Management of quarantined threats.
- **Logs:** Access to logs for scanner and protection module.
- **Ignore List:** Management of items which will be ignored by both scanner and protection module.
- **Settings:** Detailed configuration of program, scanner, database updater and task scheduler.
- **More Tools:** Provides information about other Malwarebytes protection products.
- **About:** Program version, license, and link to on-line help.

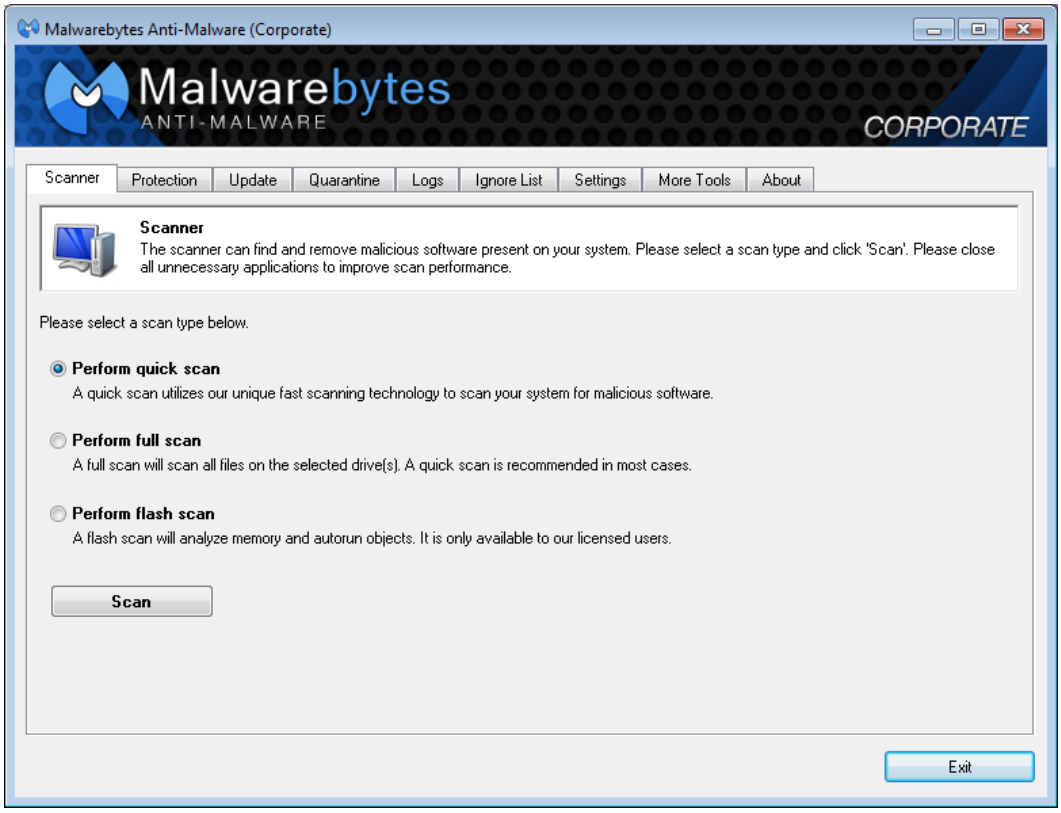
As each tab is selected, its background color will change from gray to white. The remainder of the screen is used for functionality associated with the tab.

Main Window

The main window begins immediately underneath the row of tabs, starting with a title bar to provide immediate recognition. All activities related to the selected tab occur within the boundaries of the main window. Because each aspect of the program will be discussed later in this guide, screenshots will also be included later as part of those discussions.

Scanner

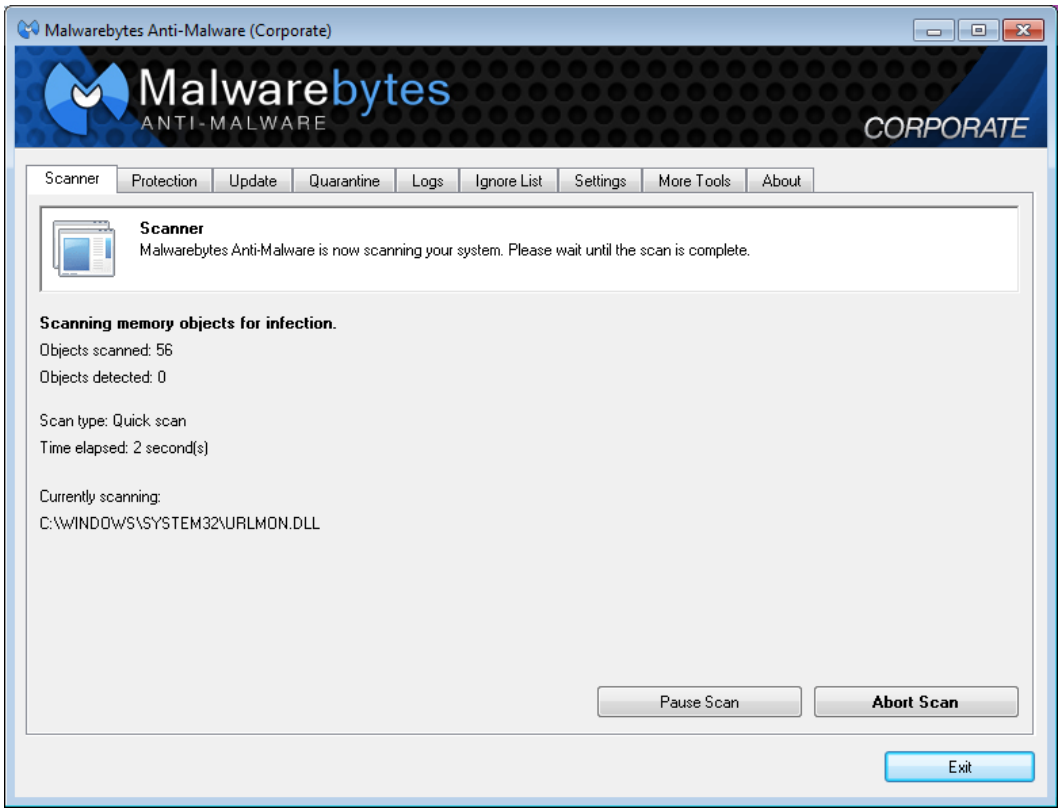
This tab provides the capability to select a method of scanning, and to execute the selected scan. A screenshot is shown below.



Malwarebytes Anti-Malware offers three methods of scanning your computer. They are:

- **Quick Scan:** Scans all system locations where malware is known to install itself. This is the scan type 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.



The amount of time required to execute a scan varies widely, depending on the type of scan and the age of the computer. 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 a computer which has been in use for an extended period of time. As a general rule, computers 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*) computer will require less time because there is less work to do.

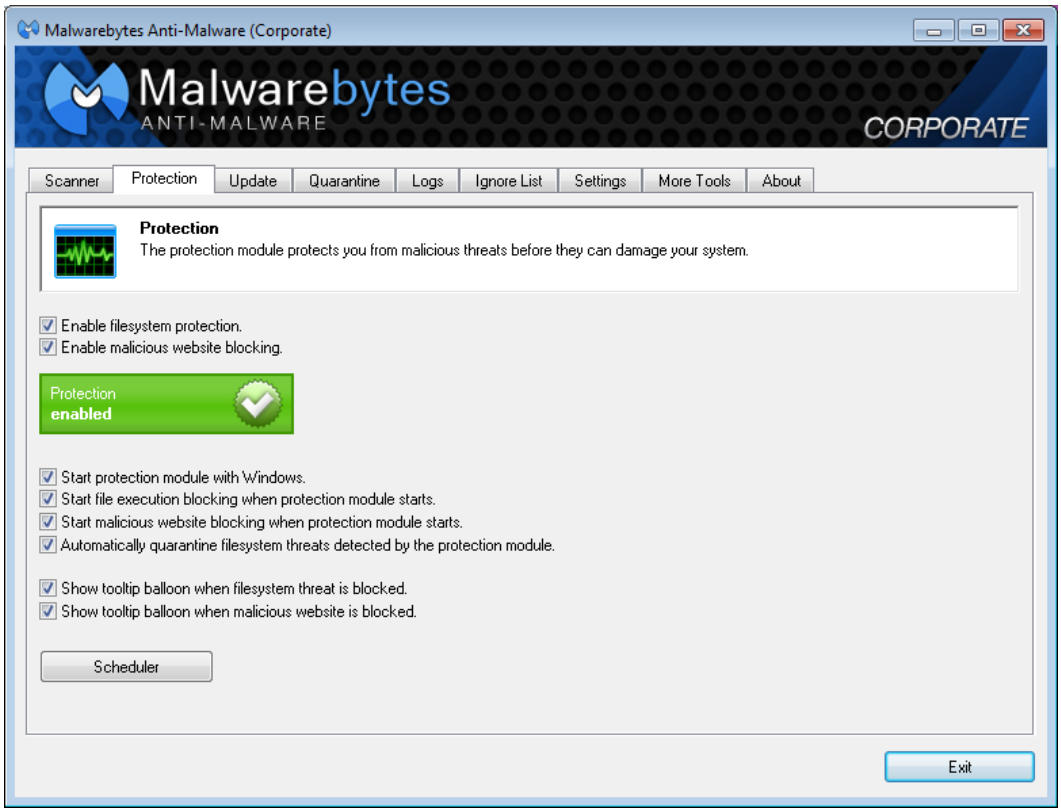
Once the scan has completed, a status message will be presented in the middle of your screen. A log which details the scan will also be displayed.

Protection

This tab controls characteristics of the Protection Module. This component is the single most important feature of *Malwarebytes Anti-Malware* It provides the capability to defend against threats proactively. Scans – whether scheduled or on demand – are reactive in nature. If a threat has made its way onto your computer, damage may have already been done by the time that a scan is executed. The Protection Module guards against threats at all times. A screenshot of the Protection tab is shown below.

NOTE 1: Settings for this tab may be overridden by instructions issued at the Windows command line. See Appendix A for further details.

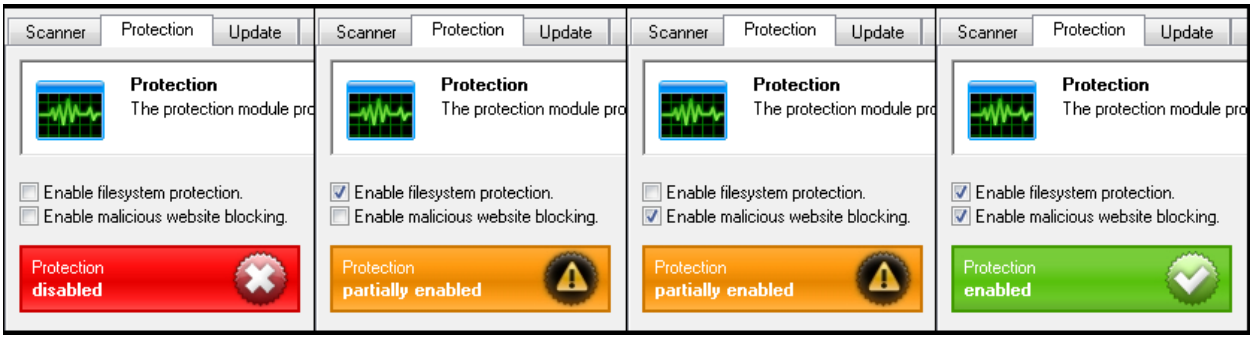
NOTE 2: A password may be required to access this tab, if a password has been set. See *Settings* (page 20) for further details on this feature.



The first thing you notice on this screen is the status of the Protection module. It is designed to stand out, and to give the user an immediate status. This is controlled by settings of the two checkboxes immediately above the status indicator. These checkboxes are:

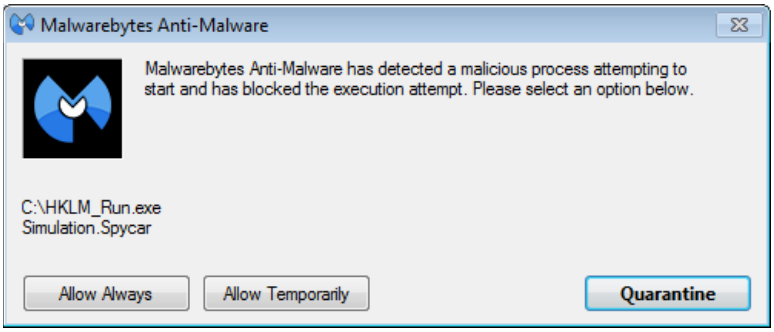
- **Enable filesystem protection:** Malicious file execution blocking is enabled. If the tray icon for the protection module is not already running, it will start and will enable both protection components if they are both set to start when the protection module starts. If the tray icon is already running, it will simply enable or disable Filesystem Protection.
- **Enable malicious website blocking:** Malicious website blocking is enabled. If the tray icon for the protection module is not already running, it will start and will enable both protection components if they are both set to start when the protection module starts. If the tray icon is already running, it will simply enable or disable Website Blocking.

Based on the settings chosen for these two checkboxes, you will see corresponding changes in the Protection Module status indicator, as shown below.

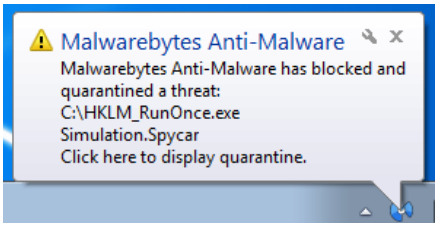


There are a number of other configuration settings which may be specified here for the Protection Module. They are as follows:

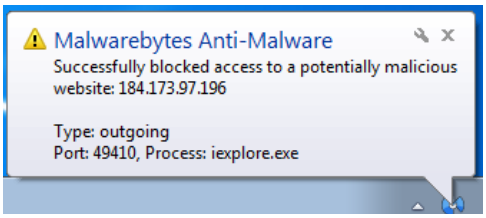
- **Start protection module with Windows:** This option will start the Protection Module during system startup and place a tray icon in the system tray.
- **Start file execution blocking when protection module starts:** This option will start the Protection Module during system startup and place a tray icon in the system tray.
- **Start malicious website blocking when protection module starts:** This option blocks access to known malicious websites.
- **Automatically quarantine filesystem threats detected by the protection module:** This option automatically quarantines infected files detected by the protection module. When this setting is disabled, the user is prompted to take an action. The three available actions are:
    - **Quarantine:** Blocks the threat from running and quarantines the file
    - **Allow Temporarily:** Allow the threat to run once only, but block it if it attempts to run at a later time
    - **Allow Always:** Add the threat to the *Ignore List*.



- **Show tooltip balloon when filesystem threat is blocked:** This option generates a tray icon notification whenever a filesystem threat is quarantined. *Automatically quarantine filesystem threats detected by the protection module* must be enabled for this option to function.



- **Show tooltip balloon when malicious website is blocked:** This option will generates a tray icon notification whenever a malicious IP address is blocked. Details such as the application name, the connection type as well as the port number are shown on Windows Vista and higher operating systems.



Following the configuration checkboxes, there is also a button which allows a direct link to **Scheduler** Settings, a subset of program **Settings**. This will be discussed in complete detail beginning on page 20.

Update

This tab provides information about the signature database which *Malwarebytes Anti-Malware* uses to provide protection, as well as allowing the user to check for updates immediately, rather than waiting for the next scheduled database update. A screenshot of this tab is shown below.

NOTE:	Settings for this tab may be overridden by instructions issued at the Windows command line. See Appendix A (beginning on page 29) for further details.

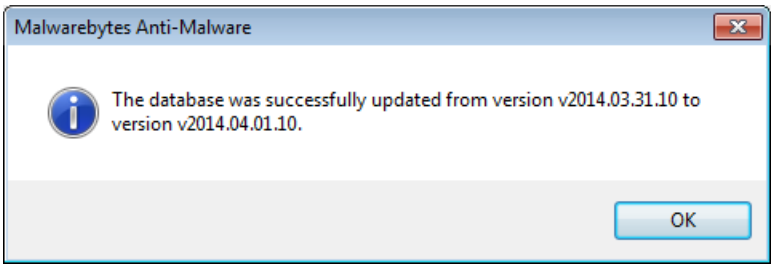
By clicking the *Check for Updates* button, *Malwarebytes Anti-Malware* will contact a Malwarebytes internet server and check for available database updates. If an update is available, it will be downloaded and merged into the program's signature database.

The *Settings* section of this guide (page 20) will provide information on how to configure *Malwarebytes Anti-Malware* to check for database updates on a scheduled basis, freeing the user from the task, and also assuring that up to date signatures are available. Updates are typically available 6-15 times daily. In most cases, updates are very small. If a computer has been unable to receive

database updates according to the defined schedule, the size of the update may be much larger, though the size of the database as a whole is in the neighborhood of ten megabytes.

Please note that if *Malwarebytes Anti-Malware* is more than fifty (50) database updates behind what is current, a full database update will occur. This method is used because it takes less time to download a full database than to process and integrate that many incremental updates.

This screen should be checked periodically to assure that signature updates are being received on a regular basis. Following a successful update, a user notification will be provided in a dialog box similar to the one shown here.

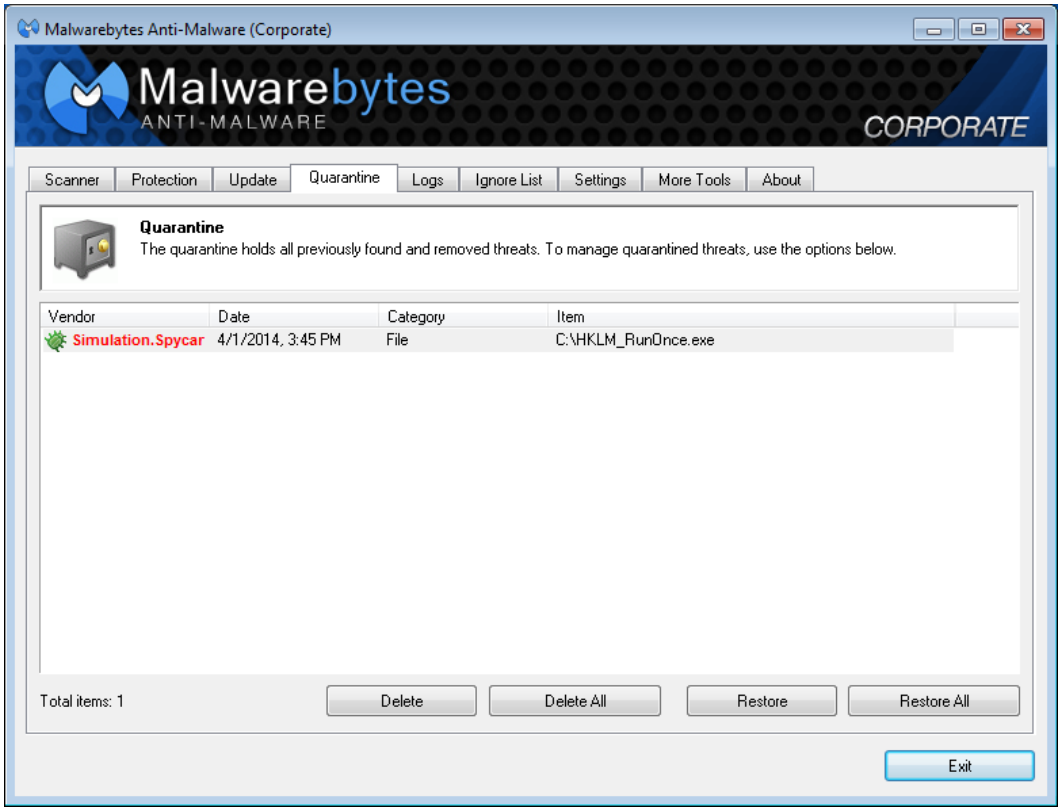


Please note that database updates are shown using the format v*yyyy.mm.dd.##*, which specifies the year, month, day, and update number released on the day listed. While the exact time of the update is not shown as part of the filename, dates shown are referenced to Greenwich Mean Time. New York's time 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.

Quarantine

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

NOTE:	Settings for this tab may be overridden by instructions issued at the Windows command line. See Appendix A for further details.



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 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:

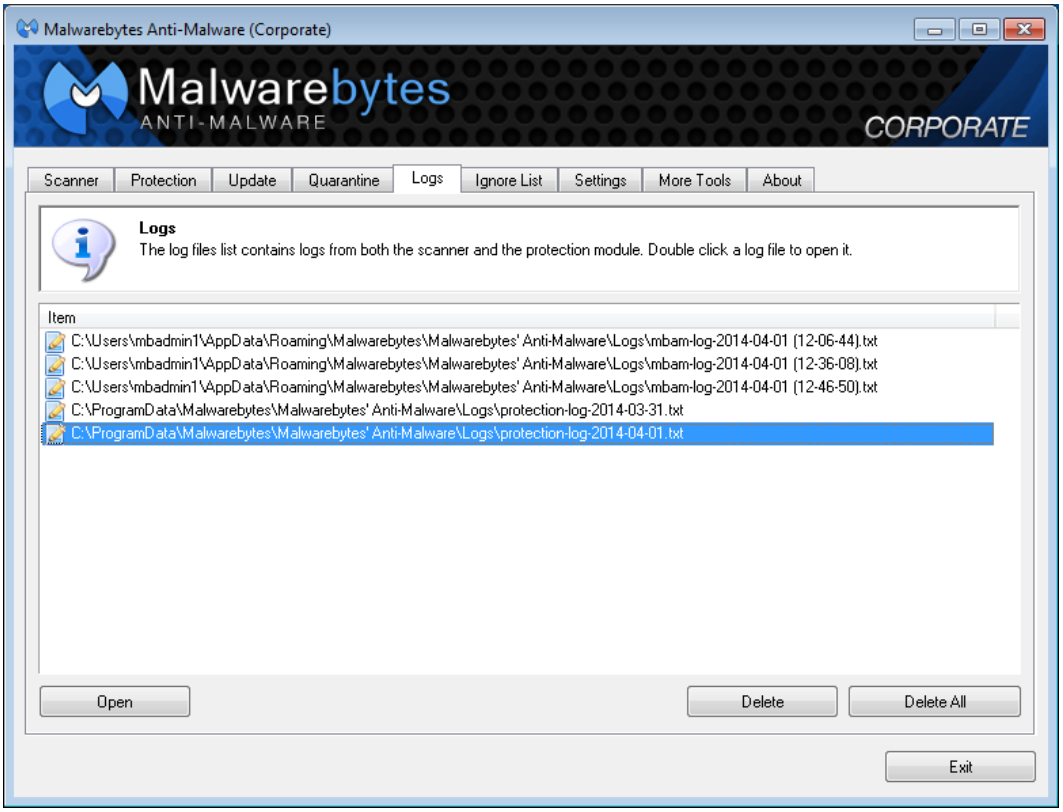
- **Delete:** Delete a file which has been selected by highlighting it.
- **Delete All:** Delete all files shown on the list
- **Restore:** Restore a file which has been selected by highlighting it.
- **Restore All:** Restore all files shown on the list

Logs

Malwarebytes Anti-Malware produces and maintains two different categories of logs during operation. This tab provides an itemization of those logs, and allows access to them as well. Log types are:

- **Protection Log:** A daily log which itemizes updates to the signature database as well as critical real-time protection events. The location of the log is shown along with the filename.
- **Scan Log:** An event log which shows program configuration and results of each scan that has been executed on the computer which Malwarebytes is installed on. The date and time of the scan encoded into the filename is based on the computer's internal clock. The location of the log is shown along with the filename.

A screenshot of the logs screen is shown here.



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.

Ignore List

The *Ignore List* is an itemization of files which are ignored by both the Protection Module and 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 *Protection* setting *Automatically quarantine filesystem threats detected by the protection module* is unchecked, and you elect to quarantine the detected file. See page 12 for further details on *Protection* settings.

NOTE 1: A password may be required to access this tab, if a password has been set. See *Settings* (page 20) for further details on this feature.

NOTE 2: Settings for this tab may be overridden by instructions issued at the Windows command line. See Appendix A (beginning on page 29) for further details.

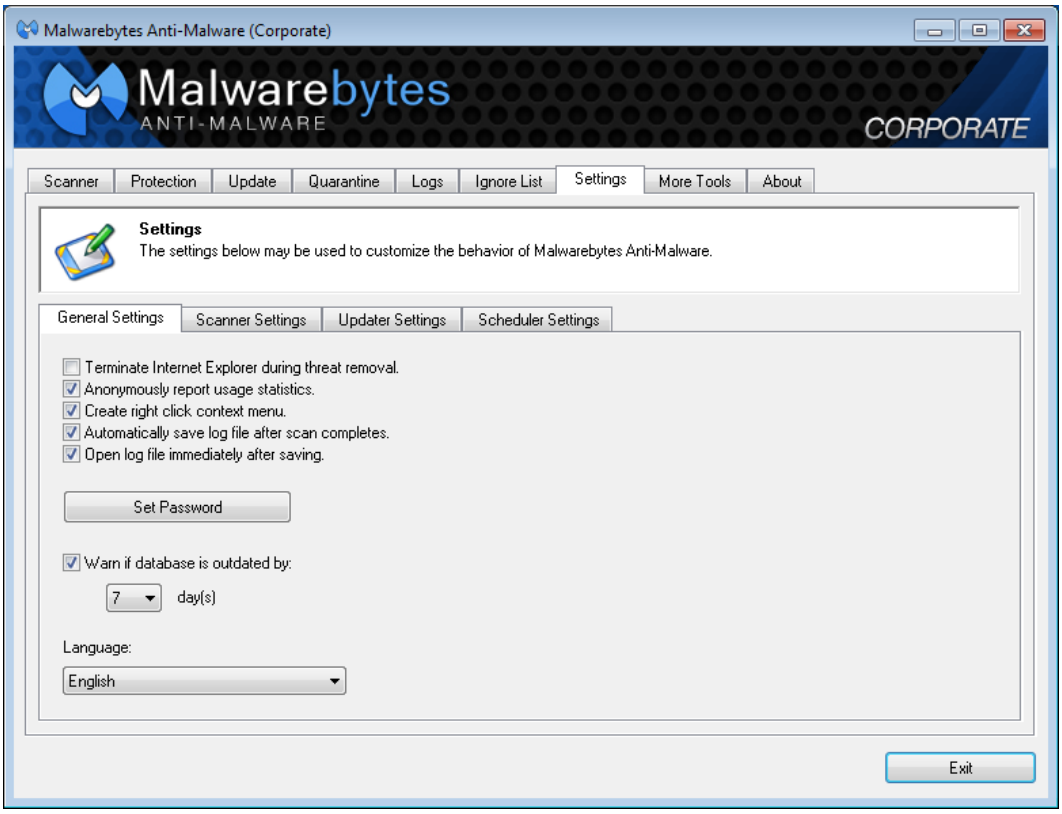
Settings

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

NOTE 1:	A password may be required to access this tab, if a password has been set.
NOTE 2:	Settings for this tab may be overridden by instructions issued at the Windows command line. See Appendix A for further details.

General Settings

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



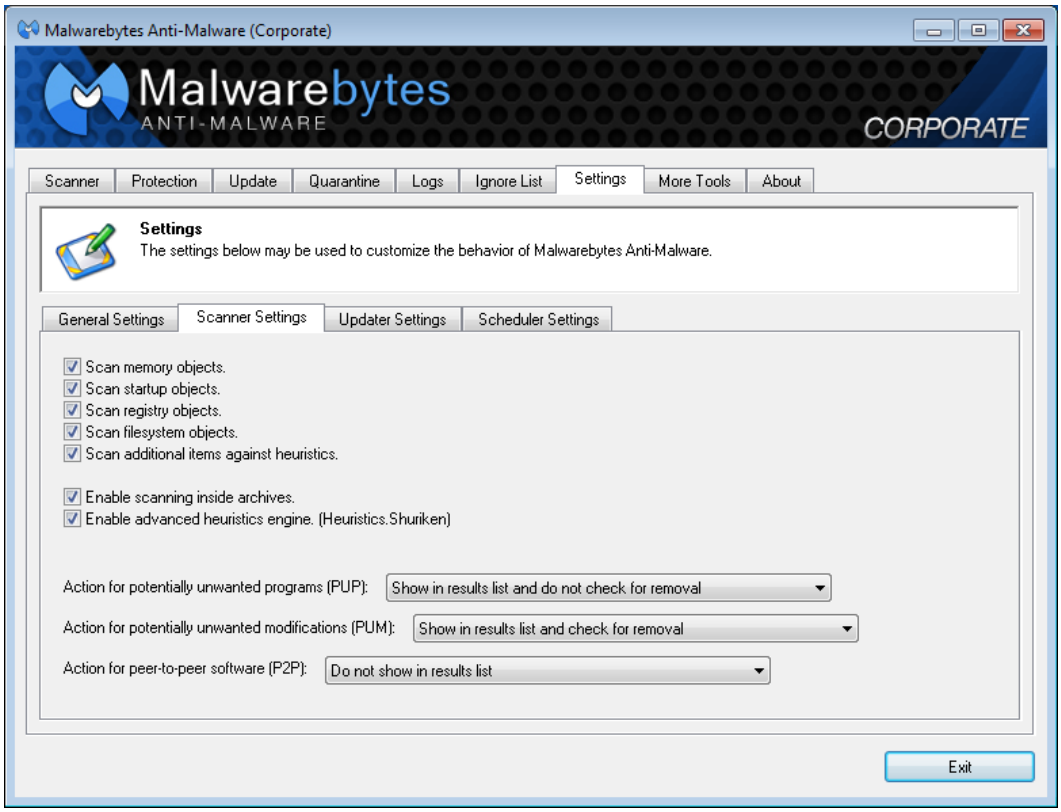
Individual settings which may be configured here are:

- **Terminate Internet Explorer during threat removal:** Enabling this option allows *Malwarebytes Anti-Malware* 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.
- **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:** When enabled, a user may right-click a file or folder to scan that file or folder.
- **Automatically save log file after scan completes:** Automatically 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 *Protection*, *Ignore List* and *Settings* tabs of the user interface.
- **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 drop-down menu allows the user to select the preferred language used within the program.

Scanner Settings

This tab controls settings which are specific to scanning functionality within the program. Settings configured here do not apply to the Protection module. A screenshot of the Scanner Settings tab is shown below.



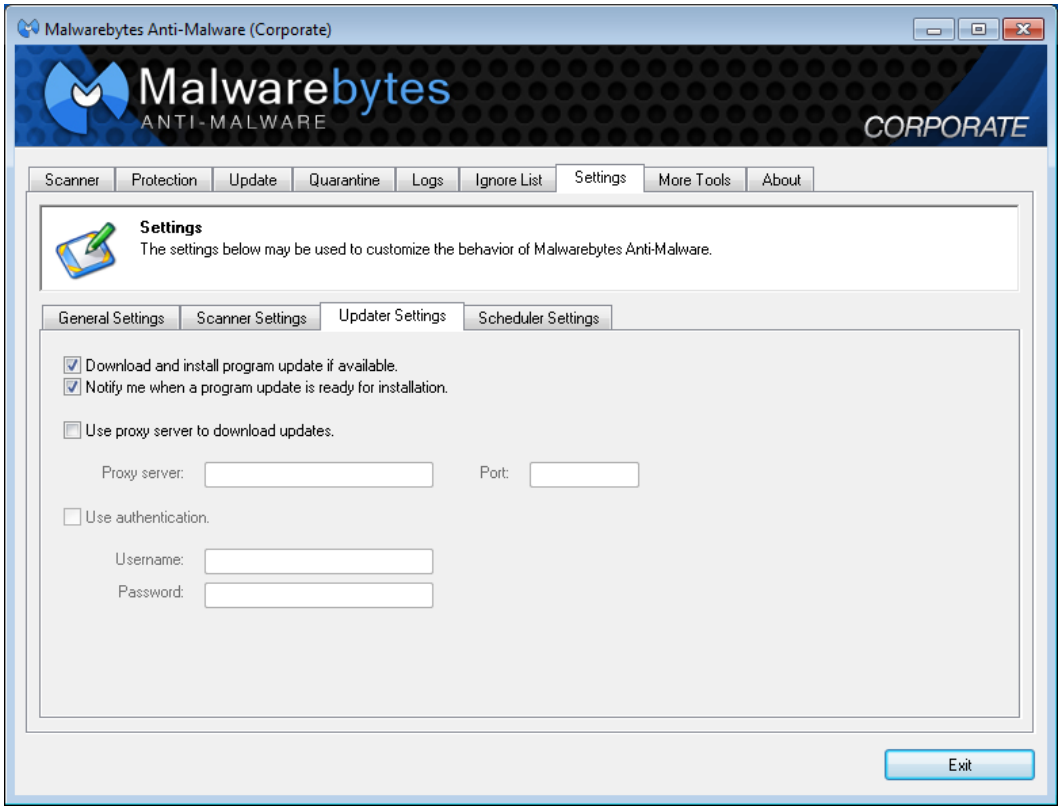
Individual settings which may be configured here are:

- **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.

Updater Settings

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

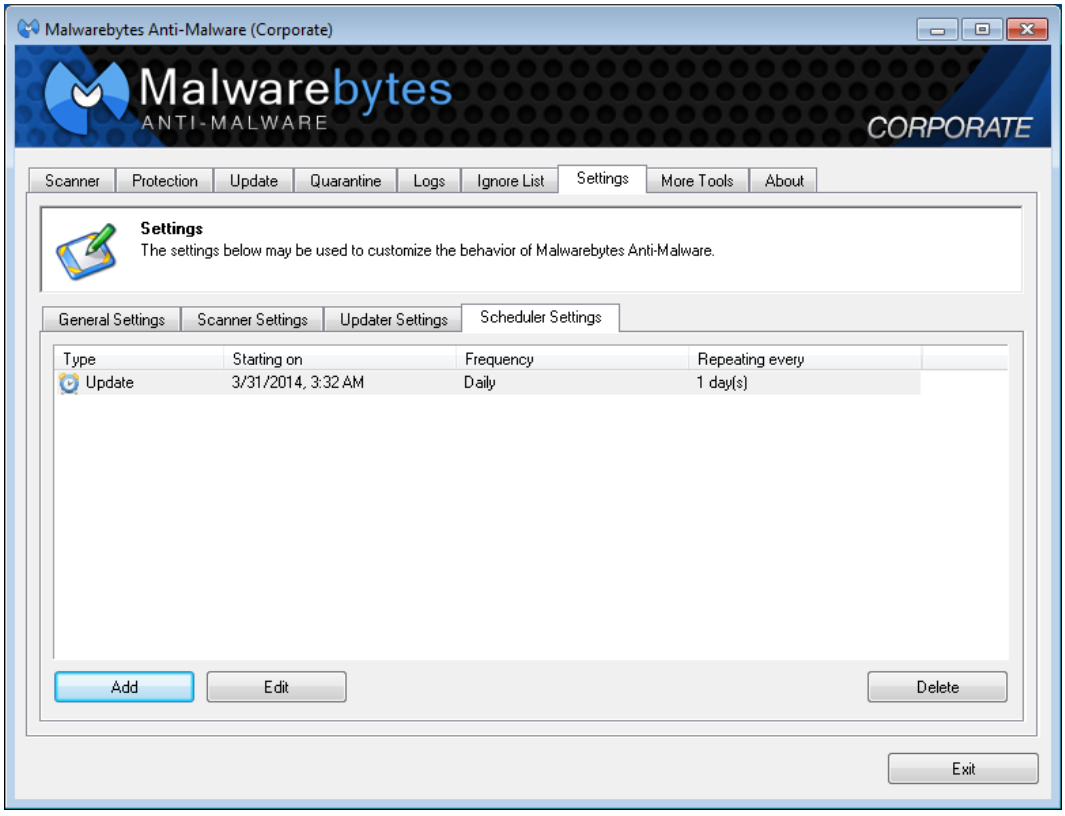


Individual settings which may be configured here are:

- **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 tray icon for the protection module will display a tooltip balloon to let the user know that a new version of *Malwarebytes Anti-Malware* 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 not used anywhere else in the program.

Scheduler Settings

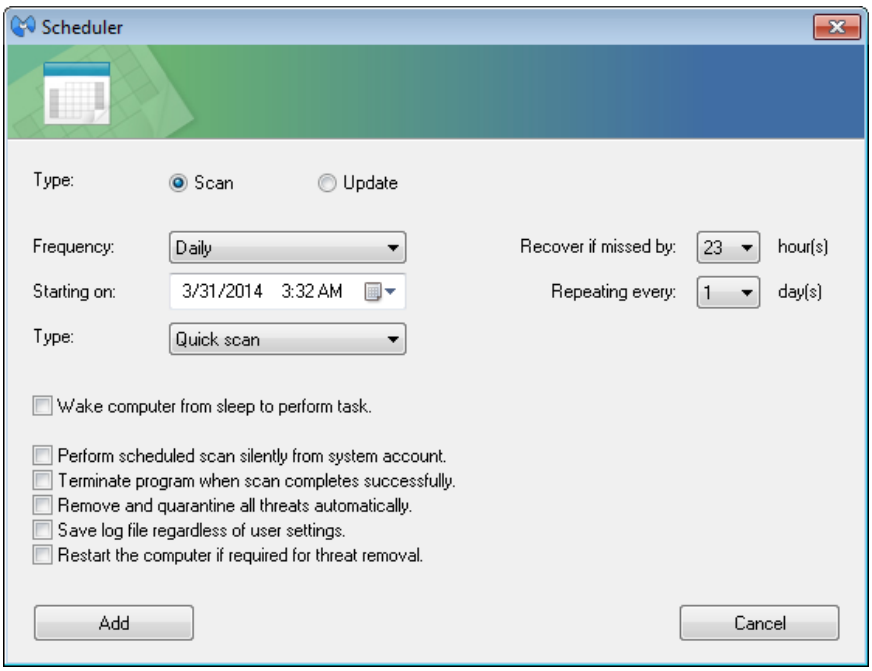
This tab provides settings pertaining to scheduling of scans and database updates. The main scheduling tab is shown below.



All scheduled tasks will be displayed in the main body of the screen as shown here. You may edit an existing task by highlighting the task and clicking **Edit**. You may delete an existing task by highlighting the task and clicking **Delete**. You may add a new task by clicking the **Add** button.

Adding a New Scheduled Scan

When the **Add** button is clicked, a *Scheduler* window opens to allow you to provide specifications for the new task. The screenshot below shows the *Scheduler* window, set to add a new scan task.



A number of scan-specific settings must be entered. A description of each setting is as follows:

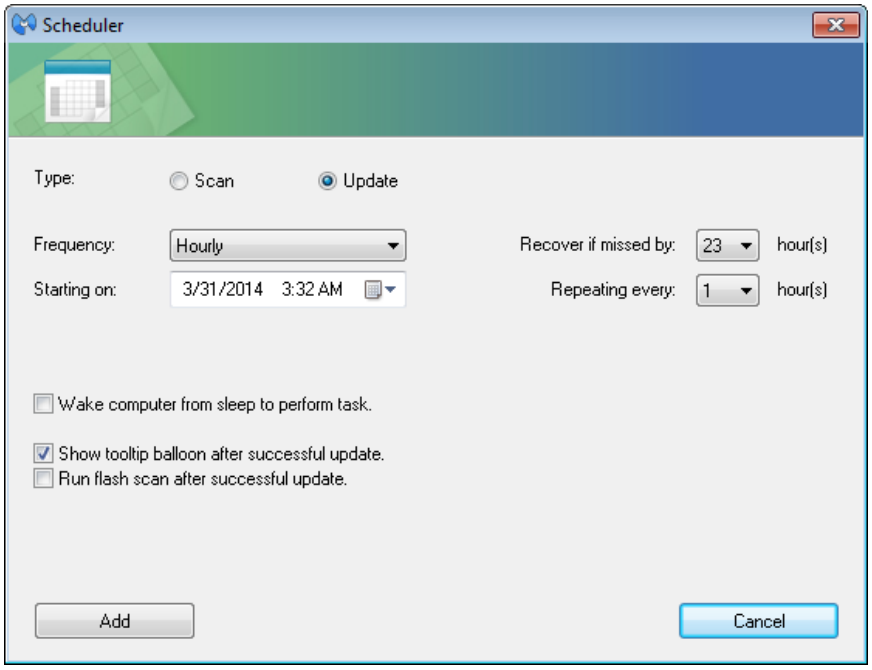
- **Frequency:** Select how often you want your scheduled scan to occur. Available options are **Hourly**, **Daily**, **Weekly**, **Monthly**, **Once**, and **On reboot**.
- **Starting on:** Choose the date and time that the scheduled scan should run for the first time. You may click in the box itself to change the date or time and you may also change the date by clicking on the small calendar icon on the right side of the box.
- **Recover if missed by:** This is set to 0 by default, but if set to any other number (1-23), the task will attempt to run if the scheduled time was missed because the system was turned off during the actual scheduled time and the system is running within the number of hours that *Recover if missed by* is set to. Example: A daily scan is set to run at 12:00AM, but your computer was not running at 12:00AM. *Recover if missed by* is set to 8 hours. If your PC is running at any time between 12:00AM and 8:00AM, the scheduled scan will execute. This option is unavailable for *monthly* and *on reboot* scans.
- **Repeating every:** Select how often the scheduled scan repeats. Available options are **1-23** hours for hourly scans, **1-60** days for daily scans, and **1-8** weeks for weekly scans. This option is unavailable for scans set to run *on reboot*.
- **Wake computer from sleep to perform task:** If your computer has Wake-On-LAN hardware capability, *Malwarebytes Anti-Malware* will attempt to wake your computer from sleep mode to execute the scheduled scan. This option is ignored if your computer cannot provide hardware functionality. This option is unavailable for scans set to run *on reboot*.
- **Perform scheduled scan silently from system account:** If checked, the scan will run from the hidden SYSTEM user account, resulting in the scan executing in the background without a scanner window showing. Upon completion of the scan, regardless of whether or not threats were found, the scan will terminate.
- **Terminate program when scan completes successfully:** If checked, *Malwarebytes Anti-Malware* will close if no threats were detected during a scan. This checkbox is automatically selected and cannot be unchecked if you have also enabled the *Perform scheduled scan silently from system account* option.
- **Remove and quarantine all threats automatically:** If checked, *Malwarebytes Anti-Malware* will remove any detected threats. Note that it also honors your scanner settings for PUP, PUM and P2P objects, so if any or all are not set to be selected for removal, they will not be removed.

- **Save log file regardless of user settings:** If checked, a log file will be saved upon completion of a scan even if *Automatically save log file after scan completes* (in *General Settings*) is unchecked.
- **Restart the computer if required for threat removal:** If checked, your computer will reboot if required to remove a threat which has been detected during a scan. **Please note** that this reboot would occur without warning, so any files open in other programs will not be saved.

Once you have defined the settings as required, click **Add** to save the newly-defined scan.

Adding a New Scheduled Update

When the **Add** button is clicked, a *Scheduler* window opens to allow you to provide specifications for the new task. The screenshot below shows the *Scheduler* window, set to add a new update task.



A number of scan-specific settings must be entered. A description of each setting is as follows:

- **Frequency:** Select how often you want your scheduled check for updates to occur. Available options are **Real-time**, **Hourly**, **Weekly**, **Monthly**, **Once**, and **On reboot**.
- **Starting on:** Choose the date and time that the scheduled update should run for the first time. You may click in the box itself to change the date or time, and you may also change the date by clicking on the small calendar icon on the right side of the box.
- **Recover if missed by:** This is set to 0 by default, but if set to any other number (1-23), the task will attempt to run if the scheduled time was missed because the system was turned off during the actual scheduled time and the system is running within the number of hours that *Recover if missed by* is set to. Example: A daily scan is set to run at 12:00AM, but your computer was not running at 12:00AM. *Recover if missed by* is set to 8 hours. If your PC is running at any time between 12:00AM and 8:00AM, the scheduled update will occur. This option is unavailable for *monthly* and *on reboot* updates.
- **Repeating every:** Select how often the scheduled update repeats. Available options are **1-59** minutes for real-time updates, **1-23** hours for hourly updates, **1-60** days for daily updates, and **1-8** weeks for weekly updates. This option is unavailable for all other frequencies.
- **Wake computer from sleep to perform task:** If your computer has Wake-On-LAN hardware capability, *Malwarebytes Anti-Malware* will attempt to wake your computer from sleep mode to execute the scheduled update. This option is ignored if your computer cannot provide hardware functionality. This option is unavailable for updates set to run *real-time* or *on reboot*.

- **Show tooltip balloon after successful update:** This option instructs the tray icon used for real-time protection to notify you when a successful update has occurred, but only if the database was actually updated. In order to receive this notification, The Protection Module must be running, however it does not require that either component of the protection module be enabled.
- **Run flash scan after successful update:** This option instructs *Malwarebytes Anti-Malware* to execute a flash scan following a successful update. It's useful for verifying that you aren't infected with anything which was not detected in the previous database but is now detected in the one which was just downloaded by the updater. This scan cannot be set to run silently.

Once you have defined the settings as required, click **Add** to save the newly-defined update.

More Tools

This tab is a showcase for several tools and products which are downloadable from the Malwarebytes website. This content is dynamically updated to offer new products.

About

This tab provides information which may be of value if you need to contact Malwarebytes Customer Success, or if you need to verify information pertaining to your *Malwarebytes Anti-Malware* installation. A screenshot of this tab is shown here.

Directly below the Malwarebytes logo, you will find the program version and build number. Below that are clickable links to access the Malwarebytes web site as well as a compiled help system. Following the abbreviated End User Licensing Agreement (EULA) is the *ID* associated with your license (masked in the above example). Your license key will be shown only by asterisks. Neither the *ID* nor *Key* will be displayed for a non-licensed installation.

Appendix A: Command Line Reference Guide

Malwarebytes Anti-Malware supports an extensive API of command line parameters. 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-setup <parameter_1>**
- Optional specifications are encased by square brackets
  Example: **mbam-setup <parameter_1> [parameter_2]**
- Repeated items are shown by a grouping of dots
  Example: **mbam-setup <parameter _1> [parameter_2] … [parameter_n]**
- Choice of specifications are separated by vertical bars
  Example: **mbam-setup <0|1|2|3>**

Commands described in this section are divided by the functional areas in which they are used. These commands 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-Malware* to operate as a task which is invisible to the computer user. When this is the case, command line tools offer the only method of modifying program configuration on the endpoint.

Installation Commands (mbam-setup.exe)

Malwarebytes Anti-Malware installation is accomplished with a single command. To assist you with first-time installation, we are also providing a few samples to help you hit the ground running. **Please note** that Malwarebytes cannot take responsibility for scripts written by customers, and cannot provide scripting advice.

Installer

Usage:

mbam-setup <*parameter_1*> ... [*parameter_n*]

Purpose:

This command controls installation of *Malwarebytes Anti-Malware* on a computer, based on parameters passed when the command is executed. The command line interface must be invoked as an Administrator to provide proper authorization for the program to install and execute properly. Anti-virus and/or other security software should be temporarily disabled prior to execution of this command. Failure to do so may result in that software blocking successful installation of Malwarebytes.

Parameters:

/dir=<path>	Specifies an alternate installation directory. If the directory does not exist, it will be created here. **Please note:** The default installation directory is: 32-bit OS: *C:\Program Files\Malwarebytes' Anti-Malware* 64-bit OS: *C:\Program Files (x86)\Malwarebytes' Anti-Malware*
/log	Causes setup to create a log file in the user's temporary directory detailing file installation and [Run] actions taken during the installation process.
/log="filename"	Causes setup to create a log file in the specified location instead of the user's temporary folder, detailing file installation and [Run] actions taken during the installation process. This should include complete path and file name. The folder must already exist.
/nocancel	Prevents the user from cancelling during installation process by disabling the *Cancel* button and ignoring clicks on the Close button. Useful along with **/silent** or **/verysilent**.
/noicons	Instructs setup not to place shortcuts in the Windows Start Menu. Can be combined with **/tasks="".**

/norestart	Instructs setup not to reboot even if necessary
/silent	
/verysilent	Instructs Setup to be silent or very silent. When Setup is silent, the wizard and the background window are not displayed but the installation progress window is displayed. When setup is very silent, the installation progress window is not displayed.
/suppressmsgboxes	Instructs setup to suppress message boxes. Only has an affect when combined with **/silent** and **/verysilent**.
/tasks=""	Instructs Setup not to place icons on the Windows desktop

Examples:

mbam-setup /silent /nocancel
mbam-setup /noicons /tasks=""
mbam-setup /verysilent /nocancel /suppressmsgboxes /norestart

Sample Batch File Installer

Malwarebytes has provided this sample script to assist you with understanding how our command line installation tools may be integrated into an installer script.

```
REM Assumes that Malwarebytes has not been installed before
@echo off
echo+
echo ** Running Malwarebytes Anti-Malware installation batch script **
%~d0
cd %~dp0
mbam-setup.exe /nocancel /norestart /verysilent /suppressmsgboxes
IF DEFINED programfiles(x86) (cd "%programfiles(x86)%\Malwarebytes' Anti-Malware") ELSE (cd "%programfiles%\Malwarebytes' Anti-Malware")
START /WAIT mbamapi.exe /register 12345-67890 AAAA-BBBB-CCCC-DDDD
START /WAIT mbamapi.exe /set hidereg on
START /WAIT mbamapi.exe /update
START /WAIT mbamapi /protection –install
START /WAIT mbamapi /protection -start
```

Sample VBScript Installer

Malwarebytes has provided this sample script to assist you with understanding how our command line installation tools may be integrated into an installer script.

```
'Sample VBScript for first-time install of Malwarebytes - Only an example - testing and modification will be required.
On Error Resume Next
strComputer = "."
Set objShell = WScript.CreateObject("WScript.Shell")
Set objFilesys = CreateObject("Scripting.FileSystemObject")
Set objWMIService = GetObject("winmgmts:\\" & strComputer)
If objFilesys.FileExists("C:\Program Files\Malwarebytes"&Chr(39)&" Anti-Malware\mbamapi.exe") Then
  objShell.Run ("""C:\Program Files\Malwarebytes"&Chr(39)&" Anti-Malware\mbamapi.exe"" /register 12345-67890 AAAA-BBBB-CCCC-DDDD"),0,True
  objShell.Run ("""C:\Program Files\Malwarebytes"&Chr(39)&" Anti-Malware\mbamapi.exe"" /protection –install"),0,True
  objShell.Run ("""C:\Program Files\Malwarebytes"&Chr(39)&" Anti-Malware\mbamapi.exe"" /protection –start"),0,True
  objShell.Run ("""C:\Program Files\Malwarebytes"&Chr(39)&" Anti-Malware\mbamapi.exe"" /update"),0,True
Else
  objShell.Run ("C:\DOWNLOADS\mbam-setup.exe" & " /verysilent /suppressmsgboxes /nocancel"),0,True
  objShell.Run ("""C:\Program Files\Malwarebytes"&Chr(39)&" Anti-Malware\mbamapi.exe"" /register 12345-67890 AAAA-BBBB-CCCC-DDDD"),0,True
  objShell.Run ("""C:\Program Files\Malwarebytes"&Chr(39)&" Anti-Malware\mbamapi.exe"" /update"),0,True
  objShell.Run ("""C:\Program Files\Malwarebytes"&Chr(39)&" Anti-Malware\mbamapi.exe"" /protection –install"),0,True
  objShell.Run ("""C:\Program Files\Malwarebytes"&Chr(39)&" Anti-Malware\mbamapi.exe"" /protection –start"),0,True
End If
Set objShell = Nothing
Set objFilesys = Nothing
Set objWMIService = Nothing
```

Configuration & Operation Commands (mbamapi.exe)

All commands of this type are performed with the *Malwarebytes Anti-Malware* API (mbamapi.exe). Because of the vast array of options which this command provides, they are listed here by function.

Define Configuration Settings

Usage:

mbamapi /set <*parameter*> <value1>[| value2| value3]

Purpose:

This command provides capability to define scan, update and operational characteristics of *Malwarebytes Anti-Malware*. Multiple parameters may be defined through use of this command, but each must be executed separately. Please note that repetitive execution does not add significant overhead. **Please note** that many configuration items defined here are referenced in other commands to be discussed later in this section.

Parameters:

terminateie <on|off>	Controls whether program will terminate Internet Explorer to remove threats during scans. Default value is off.
reportthreats <on|off>	Controls whether program will report anonymous usage statistics. Default value is on.
contextmenu <on|off>	Controls whether program can be initiated from a right click context menu in Windows Explorer. Default value is on.
autosavelog <on|off>	Controls whether a log file will be saved automatically after completion of a scan. Default value is on.
openlog <on|off>	Controls whether a log file will be opened immediately after it is saved. Default value is on.
hidereg <on|off>	Controls whether registration information is hidden on the *About* tab. Default value is off.
updatewarn <on|off>	Controls whether a warning is issued to the user if signature database is not updating. Warning is based on value of setting *updatewarndays*. Default value is on.
updatewarndays <x>	Issue a warning if database is outdated by <*x*> days. Default value is 7.
language <language_file>	Language to be used in the user interface. Available languages are those located within the Malwarebytes' Anti-Malware Languages subfolder.
alwaysscanarchives <on|off>	Controls whether archives will be scanned during scans. Default value is on.
alwaysscanmemory <on|off>	Controls whether memory objects will be scanned during scans. Default value is on.
alwaysscanstartups <on|off>	Controls whether startup objects will be scanned during scans. Default value is on.
alwaysscanregistry <on|off>	Controls whether the Windows Registry will be scanned during scans. Default value is on.
alwaysscanheuristics <on|off>	Controls whether signature-based scanning will be supplemented by heuristics. Default value is on.
advancedheuristics <on|off>	Controls whether Shuriken advanced heuristics is used as part of heuristic scanning. Default value is on.

detectpup <1|2|0>	Controls how Potentially Unwanted Programs (PUPs) are handled. Values are: **1** Detect PUPs and select for removal **2** Detect PUPs but do not select for removal [default] **0** Do not detect PUP items
detectpum <1|2|0>	Controls how Potentially Unwanted Modifications (PUMs) are handled. Values are: **1** Detect PUMs and select for removal [default] **2** Detect PUMs but do not select for removal **0** Do not detect PUMs
detectp2p <1|2|0>	Controls how Peer-to-Peer items are handled. Values are: **1** Detect P2P items and select for removal **2** Detect P2P items but do not select for removal **0** Do not detect P2P items [default]
downloadprogram <on|off>	Controls if available program updates will be downloaded and installed. Default value is on.
notifyinstallprogram <on|off>	Controls if user is notified when a downloaded program update is available for installation. Default value is on.
startwithwindows <on|off>	Controls if real-time protection is started upon Windows startup. Default value is on.
startfsdisabled <on|off>	Controls if file execution blocking is disabled when real-time protection starts. Default value is off.
startipdisabled <on|off>	Controls if malicious website blocking is disabled when real-time protection starts. Default value is off.
silentipmode <on|off>	Controls if tooltip balloon notifications are hidden when a malicious website is blocked. Default value is off.
defaultscan <0|1|2>	Controls the scan method used by default when the scanner is opened. Values are: **0** Sets quick scan as the default selected scan [default] **1** Sets full scan as the default selected scan **2** Sets flash scan as the default selected scan
fullsilentmode <on|off>	Controls whether protection module operates in Full Silent mode. This mode gives no visual indications when threats are blocked and/or quarantined, and there is no visible tray icon. Default value is off.
limitedusermode <on|off>	Controls if program executes in limited user mode. In this mode, user has no access to disable/exit protection module, modify settings, Ignore List or Quarantine. Default value is off.
autoquarantine <on|off>	Controls whether protection module will automatically quarantine detected threats. Default value is on.
autoquarantinenotify <on|off>	Controls whether a tooltip balloon notification is displayed in the system tray when a threat is automatically quarantined. Default value is on.
tsdefaultallow <on|off>	Controls whether protection module will allow threats by default. Default value is off.
randomizeupdates [x|off]	Randomizes the exact time (in seconds, specified by <*x*>) at which scheduled updates will occur, referenced to a base time. Default value is off.

delayguistart delay|off	Delay startup of protection module by <*x*> seconds following Windows startup. Default value is off.
disableipblocklogging <on|off>	Disable logging of malicious website blocks in protection logs. Default value is off.
limitupdatelogging <on|off>	Controls whether update attempts will be logged when there are no updates available for download. Errors and updates will still be logged. Default value is off.
selectedrives <spec|all>	Specifies which drives will be scanned during Full scans. Drive letters may be specified in the format **"A:|C:|D:|"** or **A:\C:\D:**. If **all** is used, that will result in C:\ being specified as the selected drive.
schedulerqueue	While you can set this value here, we recommend that you use the **/schedule** and **/unschedule** commands as documented in the *Schedule a Scan* and *Schedule a Update* sections of this appendix. For information on how to import and export this setting, refer to the *Import Configuration Settings* and *Export Configuration Settings* topics (page 43) of this document.

Schedule a Scan

Usage:

mbamapi /schedule <type> <option_1> […option_n]

Purpose:

This command adds a scheduled scan to the task scheduler. Scan options are appended to the command to tailor the scan to specific needs.

Parameters:

type	Type of scan to be added to the scheduler. Values are: **-quick** Add a quick scan to the task scheduler **-full** Add a full scan to the task scheduler. This option will check the value of *selectedrives* to determine which locations to scan. Please see *Define Configuration Settings* for further specifications of this parameter. **-flash** Add a flash scan to the task scheduler
-log	Overrides the *Save Log* checkmark on the *Settings* tab. If *Automatically Save Log After Scan Completes* is unchecked, a log file will still be saved when **-log** parameter is used.
/silent	Hides the GUI while scanning; Does not need to be used with *-terminate* as the program will always terminate after a silent scan completes.
-reboot	Reboots the computer if necessary; Only valid if *-remove* is used
-remove	Automatically removes threats and saves a log file. Unless */silent* is specified, GUI stays open.
/hourly	Configures the scan to be performed hourly. Valid range for */every* is 1-48.
/daily	Configures the scan to be performed daily. Valid range for */every* is 1-60.
/weekly	Configures the scan to be performed weekly. Valid range for */every* is 1-8.
/monthly	Configures the scan to be performed monthly. The */every* switch is invalid for monthly scans.
/once	Configures the scan to be performed only once and only at the time specified by */starting*.
/onreboot	Configures the scan to be performed every time the computer boots.

/starting Configures the start time for the first run of the scheduled item in the format *mm/dd/yyyy hh:mm:ss*.

/random Configures the scan to run at a random time. Only valid for scans set to hourly or daily, and randomizes the minute and second (for hourly scans) or hour and minute (for daily scans).

/every <x> Sets the number for the frequency of the scan to occur, i.e. for hourly, it would be 1 for every one hour and for daily it would be 2 for every 2 days. This switch is required for every option except */monthly, /once* and */onreboot*. Valid numbers for hourly scans are 1-48, representing the number of hours between each scan. Valid numbers for daily scans are 1-60, representing the number of days between each scan. Valid numbers for weekly scans are 1-8, representing the number of weeks between each scan.

/wakefromsleep Configures the scan to attempt to wake the computer from a sleep state in order to launch the scan.

/recover <x> Sets the number for the */scan* to attempt to launch again if the computer was not running when the scan was originally set to run. For example, a computer with a scan set to run at 12:00AM with a recover setting of 8 will attempt to run the scan if the computer becomes available at any point between 12:00AM and 8:00AM. The valid time range can be anywhere from 0 to 23 hours. The */recover* switch is invalid for items set to run /onreboot.

/xml Sets the scan to create an XML format log instead of a standard plain text log.

Examples:

mbamapi /schedule /scan -quick -remove -terminate -log /daily /starting 08/10/2010 23:00:00 /every 1 /silent /wakefromsleep /recover 3 /xml

Schedule a Database Update

Usage:

mbamapi /schedule /update <type> <option_1> […option_n]

Purpose:

This command adds a rules database update to the task scheduler. Update options are appended to the command to tailor the update to specific needs.

Parameters:

/silent Configures the update not to show a balloon tooltip notification after a successful update.

/realtime Configures the update to occur in realtime, checking for updates every <*x*> minutes according to how the */every* setting is configured. The */starting* switch is not to be used with */realtime* as the current time is always assumed for when to begin */realtime* updates. Valid numbers for */every* for realtime updates are 1-59.

/hourly Configures the update to be performed hourly. Valid range for */every* is 1-48.

/daily Configures the update to be performed daily. Valid range for */every* is 1-60.

/weekly Configures the update to be performed weekly. Valid range for */every* is 1-8.

/monthly Configures the update to be performed monthly. The */every* switch is invalid for monthly updates.

/once Configures the update to be performed only once, and only at the time specified by */starting*.

/onreboot Configures the update to be performed every time the computer boots.

/starting Configures start time for the first run of the scheduled item, in the format *mm/dd/yyyy hh:mm:ss*.

/random Configures the update to run at a random time. Only valid for updates set to hourly or daily and randomizes the minute and second (for hourly updates) or hour and minute (for daily updates).

/every <x> Sets the repetition factor at which update checks are performed. Valid values are 1-59 minutes (realtime updates), 1-48 hours (houly updates), 1-60 days (daily updates), and 1-8 weeks (weekly updates).

/wakefromsleep Configures the update to attempt to wake the computer from a sleep state in order to launch the update. This option is not valid for updates set to */realtime*.

/recover <x> Sets the number for the update to attempt to launch again if the computer was not running when the update was originally set to run. For example, a computer with an update set to run at 12:00AM with a recover setting of 8 will attempt to run the update if the computer becomes available at any point between 12:00AM and 8:00AM. The valid time range can be anywhere from 0 to 23 hours. The */recover* switch is invalid for items set to run */onreboot*.

/flash Configures the program to immediately launch a flash scan to check for threats after a successful database download and update. This scan cannot be configured with other options like *-silent*, *-remove*, *-reboot –terminate* etc., and will always show the scanner UI even if the scheduled update itself uses the *-silent* switch.

Examples:

mbamapi /schedule /update /flash /realtime /every 5

Remove a Scheduled Scan/Update

Usage:

mbamapi /unschedule <type><option_1> […option_n]

Purpose:

This command removes one or more scheduled tasks from the scheduler. Individual scans or updates must be specified using the exact switches which were used to create the scan or update, and may not be removed through use of the */all* switch. For individual scans and updates, please refer to the previous two commands for formatting specifications.

Parameters:

type Type of task to remove from the scheduler. Values are:

- **/all** All tasks
- **/scan** Scan tasks only
- **/update** Update tasks only

option_n If type = */all*, values for option_1 are ***blank***, ***-update***, or ***–scan***. If type is */scan* or */update*, please refer to previous two sections for formatting specifications related to individual scans/updates.

Examples:

mbamapi /unschedule /all
mbamapi /unschedule /all -scan
mbamapi /unschedule /all -update
mbamapi /unschedule /scan -quick -remove -terminate -log /daily /starting 04/10/2014 23:00:00 /every 1 /silent
mbamapi /unschedule /update /flash /realtime /every 5

Perform a Scan

Usage:

mbamapi /scan <type> <switches>

Purpose:

This command activates the *Malwarebytes Anti-Malware* client on a computer, without displaying the main dialog box.

Parameters:

type	Type of scan to be executed. Values are: **-quick** Execute a quick scan. **-full** Execute a full scan. This option will check the value of *selectedrives* to determine which locations to scan. Please see *Define Configuration Settings* for further specifications of this parameter. **-flash** Execute a flash scan.
-terminate	Close program after a scan completes if no threats were found. If a threat is detected, the program remains open so that the user can decide whether to remove the threat(s). This switch cannot be used with ***-silent***.
-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*** as the program will always terminate after a silent scan completes.
-remove	Automatically removes threats and saves a log file. GUI will remain open unless **-silent** is specified.
-reboot	Reboots the computer if necessary; Switch is valid only if ***-remove*** is used.
/xml	Sets the scan to create an XML format log instead of a standard plain text log.

Examples:

mbamapi /scan
mbamapi /scan -full
mbamapi /scan -flash -terminate
mbamapi /scan -quick -log -silent -remove -reboot /xml

Product Activation

Usage:

mbamapi /register <*id*> <*key*>

Purpose:

This command activates the *Malwarebytes Anti-Malware* client on a computer, without displaying the main dialog box.

Parameters:

id	License ID assigned by Malwarebytes for this specific computer.
key	License key assigned by Malwarebytes for this specific computer.

Examples:

mbamapi /register 12345-67890 AAAA-BBBB-CCCC-DDDD

Set/Change Password

Usage:

mbamapi /setpassword <*password*>
mbamapi /setpassword <*old_password*> <*new_password*>

Purpose:

This command sets or changes the password used to access certain features of the product. Double quotes (") are required around the password if it contains non-alphanumeric characters. **Please note** that a double quote (") is not allowed within the password itself due to its use as a delimiter.

Parameters:

password	Password assigned by admin to computer/site/user/admin.
old_password	
new_password	

Examples:

mbamapi /setpassword "malwarebytes"	Sets the password to *malwarebytes*
mbamapi /setpassword "newpw" "oldpw"	Changes the password from *oldpw* to *newpw*
mbamapi /setpassword "P^&#2@"	Sets the password to *P^&#2@*

Remove Password

Usage:

mbamapi /clearpassword <*password*>

Purpose:

This command removes the password. User must specify the existing password as authorization to execute the command. There is no command line function for removing or resetting a password if it has been lost, forgotten or misplaced. In such scenarios, a clean reinstall is required.

Parameters:

password	Existing password assigned by admin.

Examples:

mbamapi /clearpassword <password>

Proxy Configuration

Usage:

mbamapi.exe /proxy [*server*] [*port*] [*username*] [*password*]

Purpose:

This command allows *Malwarebytes Anti-Malware* to update through a proxy server. If the proxy server is configured to require authentication, <*username*> and <*password*> must be supplied. To remove previously-defined proxy settings, issue this command without any modifiers.

Parameters:

server	IP address or fully-qualified domain name of a proxy server used in the corporate network.
port	Port number used by the proxy server for communications.
username	Username which may be required to validate proxy server usage.
password	Password associated with [username].

Examples:

mbamapi.exe /proxy	Clears proxy settings
mbamapi.exe /proxy proxy.com 80	Defines proxy use without authentication
mbamapi.exe /proxy proxy.com 80 admin password	Defines proxy use with authentication

Set/Change Log File Location

Usage:

mbamapi /logtofolder [*path*]

Purpose:

This command defines or changes the disk directory where log files will be stored. If the directory does not exist, *Malwarebytes Anti-Malware* will attempt to create it. If [*path*] is blank, the directory will revert to default settings. Please note that logs created by the protection module will be saved to the location specified here.

Parameters:

path Disk location where logs will be stored. If blank, log file location will revert to default settings.

Examples:

mbamapi /logtofolder C:\mbam_logs	Set log folder to *c:\mbam_logs*
mbamapi /logtofolder	Revert log folder to default settings

Set/Change Log File Name

Usage:

mbamapi /logtofile [*path*]\[*file*]

Purpose:

This command allows the user to save all log files to the specified file. If this file does not exist, *Malwarebytes Anti-Malware* attempts to create it. The path to the log file must already exist and this setting has no effect on protection logs created by the protection module. If [file] is blank, changes revert to default settings. Newest entries are appended to top of the file. This log will not be listed in the *Logs* tab of *Malwarebytes Anti-Malware*. **Note:** If using XML logging via the **/xml** switch referred to in the *Scheduled Updates and Scans* and *Performing Scans* sections of this document, you must specify the file extension as .xml instead of .txt.

Parameters:

path Disk folder where [*file*] is/will be located. [*path*] must already exist, unless both [*path*] and [*file*] are blank.

file File name to which log files will be saved. If blank, log file name will revert to the default.

Examples:

mbamapi /logtofile C:\mbam_logs\mbam-log.txt	Save to mbam-log.txt (text format)
mbamapi /logtofile C:\mbam_logs\mbam-log.xml	Save to mbam-log.xml (XML format)
mbamapi /logtofile	Revert to default

Update Signature Database

Usage:

mbamapi /update

Purpose:

This command attempts to silently update *Malwarebytes Anti-Malware* and its signature database.

Parameters:

none

List Contents of Quarantine

Usage:

mbamapi /quarantine -list

Purpose:

This command lists the contents of the quarantine. Items stored here have been isolated from other system components so that they may not cause damage.

Parameters:

none

Delete Items from Quarantine

Usage:

mbamapi /quarantine –delete <*class*> [*specification*]

Purpose:

This command deletes items from Quarantine.

Parameters:

class <type> Type of threat to be deleted from quarantine.

Specifications for <*class*> items:

- **all** All quarantined threats
- **file** File "<drive>\<dir>\<file>", where string is enclosed in double quotes.
- **folder** Folder "<drive>\<dir>", where string is enclosed in double quotes.
- **key** Registry entry "<hive>\<key>", where string is enclosed in double quotes.
- **value** Registry value "<hive>\<key>|<value>", where string is enclosed in double quotes.

Examples:

mbamapi /quarantine -delete file "C:\Windows\file.exe"
mbamapi /quarantine -delete folder "C:\Windows\folder"
mbamapi /quarantine -delete key "HKLM\Software\key"
mbamapi /quarantine -delete value "HKLM\Software\key|value"
mbamapi /quarantine -delete all

Restore Items from Quarantine

Usage:

mbamapi /quarantine –restore <*class*> [*specification*]

Purpose:

This command restores items which have been quarantined by *Malwarebytes Anti-Malware*. **Please note** that a reboot is usually required before a quarantined item may be restored, due to *Delete On Reboot* technology used by the program.

Parameters:

class <type> Type of threat to be deleted from quarantine.

Specifications for <*class*> items:

- **all** All quarantined threats
- **file** File "<drive>\<dir>\<file>", where string is enclosed in double quotes.
- **folder** Folder "<drive>\<dir>", where string is enclosed in double quotes.
- **key** Registry entry "<hive>\<key>", where string is enclosed in double quotes.
- **value** Registry value "<hive>\<key>|<value>", where string is enclosed in double quotes.

Examples:

mbamapi /quarantine -restore file "C:\Windows\file.exe"
mbamapi /quarantine -restore folder "C:\Windows\folder"
mbamapi /quarantine -restore key "HKLM\Software\key"
mbamapi /quarantine -restore value "HKLM\Software\key|value"
mbamapi /quarantine -restore all

List Contents of Ignore List

Usage:

mbamapi /ignore -list

Purpose:

This command removes all contents from the Ignore List. Once removed, all items are again subject to scanning and real-time protection mechanisms. The Ignore List is stored in a file named exclusions.dat, and may be deployed from one system to another, as documented in *Exporting Configuration Settings* and *Importing Configuration Settings* (later in this appendix). The Ignore List is stored in the following folder:

Windows XP:
C:\Documents and Settings\All Users\Application Data\Malwarebytes\Malwarebytes' Anti-Malware
Vista, Windows 7, Windows 8:
C:\ProgramData\Malwarebytes\Malwarebytes' Anti-Malware

Parameters:

none

Add Item to Ignore List

Usage:

mbamapi /ignore –add <*class*> [*specification*]

Purpose:

This command adds items to the Ignore List. Scanning exclusions may be applied to classes **file**, **folder**, **key** and **value**. Malicious file execution blocking exclusions may be applied to classes **file** and **folder**. Malicious website blocking exclusions may be applied to class **ip**. Changes made by this command will not go into effect until ***mbamapi /reloadignore*** is executed.

> **WARNING:** Adding files, folders, registry keys, or IP addresses to your Ignore List will prevent any future detections by the program, which may lead to an infection. In most cases if the program is blocking, it is doing it for a valid reason. If in doubt, please contact Malwarebytes Customer Success for further guidance.

Parameters:

class <type> Type of item to be added.

Specifications for <*class*> items:

- **file** File "<drive>\<dir>\<file>", where string is enclosed in double quotes.
- **folder** Folder "<drive>\<dir>", where string is enclosed in double quotes.
- **key** Registry entry "<hive>\<key>", where string is enclosed in double quotes.
- **value** Registry value "<hive>\<key>|<value>", where string is enclosed in double quotes.
- **ip** IP address, in format "nnn.nnn.nnn.nnn", enclosed in double quotes.

Examples:

```
mbamapi /ignore -add file "C:\Windows\file.exe"
mbamapi /ignore -add folder "C:\Windows\folder"
mbamapi /ignore -add key "HKLM\Software\key"
mbamapi /ignore -add value "HKLM\Software\key|value"
mbamapi /ignore -add ip "111.222.33.444"
```

Remove Item from Ignore List

Usage:

mbamapi /ignore –remove <*class*> [*specification*]

Purpose:

This command removes items from the Ignore List. Once an item has been removed from the list, it is subject to scanning and real-time protection mechanisms. Changes made by this command will not go into effect until ***mbamapi /reloadignore*** is executed.

Parameters:

class <type> Type of item to be removed.

Specifications for <*class*> items:

- **file** File "<drive>\<dir>\<file>", where string is enclosed in double quotes.
- **folder** Folder "<drive>\<dir>", where string is enclosed in double quotes.
- **key** Registry entry "<hive>\<key>", where string is enclosed in double quotes.
- **value** Registry value "<hive>\<key>|<value>", where string is enclosed in double quotes.
- **ip** IP address, in format "nnn.nnn.nnn.nnn", enclosed in double quotes.

Examples:

```
mbamapi /ignore -remove file "C:\Windows\file.exe"
mbamapi /ignore -remove folder "C:\Windows\folder"
mbamapi /ignore -remove key "HKLM\Software\key"
mbamapi /ignore -remove value "HKLM\Software\key|value"
mbamapi /ignore -remove ip "111.222.33.444"
```

Reload Ignore List

Usage:

mbamapi /reloadignore

Purpose:

This command reloads any changes which have been made to the Ignore List. Changes which have been made are not effective until this command has been executed.

Parameters:

none

Protection Module Operations

Usage:

mbamapi /protection <option> [type]

Purpose:

This command controls operations related to the Protection Module, which is used to provide various type of real-time protection for *Malwarebytes Anti-Malware*.

Parameters:

-install Installs protection module; Only needed following installation/activation of product with license, or if protection module has been uninstalled

-uninstall Uninstalls protection module, removing its services and startups

-start Starts protection module. Settings specified with **startfsdisabled** and **startipdisabled** are honored.

-stop Stops all components of the protection module. Protection module will start again on reboot unless **startwithwindows** has been set to off.

-getstate Returns current status of the protection module

Return Values:

all	All protection components are enabled
none	All protection components are disabled
fs	Only file system protection is enabled
ip	Only website blocking is enabled

-enable <type> Enables selected component of the protection module. Upon a system restart, **startfsdisabled** and **startipdisabled** will be honored regardless.

Type:

fs	File system protection
ip	Website blocking

-disable <type> Disabled selected component of the protection module. Upon a system restart, **startfsdisabled** and **startipdisabled** will be honored regardless.

Type:

fs	File system protection
ip	Website blocking

Examples:

```
mbamapi /protection -install
mbamapi /protection -uninstall
mbamapi /protection -start
mbamapi /protection -stop
mbamapi /protection -getstate
mbamapi /protection -enable fs
mbamapi /protection -disable ip
```

Export Configuration Settings

Usage:

mbamapi /export all|<setting> <file>

Purpose:

This command allows *Malwarebytes Anti-Malware* settings to be exported to configuration file *settings.dat*, which may be imported into other *Malwarebytes Anti-Malware* installations. This method is typically used when one installation has been fine-tuned to provide specific performance characteristics to be replicated to all other Malwarebytes products on site. When created, the file will be stored in the following location:

Vista/Windows 7/Windows 8: **%programdata%\Malwarebytes\Malwarebytes' Anti-Malware**
Windows XP: **%allusersprofile%\Application Data\Malwarebytes\Malwarebytes' Anti-Malware**

This file is suitable for use with network management tools and Active Directory Group Policy updates.

Parameters:

setting If all configuration items are not being exported, setting may represent any configuration setting which has been previously specified.

file Valid path and filename which configuration settings will be exported to.

Examples:

mbamapi /export schedulerqueue "%userprofile%\desktop\schedule.dat"

*This exports setting for **schedulerqueue** from the registry to file* schedule.dat *on the user desktop.*

mbamapi /export reportthreats "%systemdrive%\export.dat"

*This exports registry setting **reportthreats** to file export.dat in the root of the system drive (usually C:\).*

mbamapi /export all "C:\Documents and Settings\username\Desktop\export.dat"

This exports all current program settings to file export.dat on the user desktop.

Import Configuration Settings

Usage:

mbamapi /import all|<setting> <file>

Purpose:

This command allows *Malwarebytes Anti-Malware* settings to be imported from a configuration file named *settings.dat*, which was previously created by execution of the **/export** command on another *Malwarebytes Anti-Malware* installation. This file will be automatically imported when either the scanner or protection module execute. The file will be stored in the following location:

Vista/Windows 7/Windows 8: **%programdata%\Malwarebytes\Malwarebytes' Anti-Malware**
Windows XP: **%allusersprofile%\Application Data\Malwarebytes\Malwarebytes' Anti-Malware**

Parameters:

setting If all configuration items are not being imported, setting may represent any configuration setting which has been previously specified.

file Valid path and filename which configuration settings will be imported from.

Examples:

mbamapi /import schedulerqueue "%userprofile%\desktop\schedule.dat"

*This imports setting for **schedulerqueue** from file* schedule.dat *(located on the user desktop) to the registry.*

mbamapi /import reportthreats "%systemdrive%\export.dat"

*This imports registry setting **reportthreats** from file export.dat in the root of the system drive (usually C:\).*

mbamapi /import all "C:\Documents and Settings\username\Desktop\export.dat"

This imports all current program settings from file export.dat on the user desktop.

Legacy Commands (mbam.exe)

Most command-line functionality used within *Malwarebytes Anti-Malware* has been updated to take advantage of the Malwarebytes Anti-Malware API (mbamapi.exe). There is one command which has not been migrated, because its purpose is limited to troubleshooting and is not designed to provide added functionality for the *Malwarebytes Anti-Malware* user. It is described here.

Usage:

mbam <parameter>

Purpose:

This command provides information which may be of value when troubleshooting issues with *Malwarebytes Anti-Malware*. There will likely not be a reason to execute this command unless directed to do so by Malwarebytes Technical Support.

Parameters:

/errorsilent	Suppresses all critical errors and writes the last error to <*root-drive*>*mbam-error.txt* where <*root-drive*> is the hard drive where Windows is installed.
/developer	Allows *Malwarebytes Anti-Malware* to execute a scan which creates a log containing encrypted information for use by Malwarebytes researchers. This is typically used for reporting false-positives, and allows researchers to determine why an item is being detected during the scan. When using this option, the subsequent scan must be executed using the program's user interface, and cannot be executed via the command line or scheduler. **Please note** that this option is valid for a single scan only, and will revert to standard mode following execution of the single scan.

Example:

mbam /errorsilent
mbam /developer