

**Malwarebytes Anti-Malware**  
**Users Guide**  
Version 2.0.1  
07 April 2014



## Notices

---

Malwarebytes products and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. You may copy and use this document for your internal, reference purposes only.

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.

The Malwarebytes logo and Malwarebytes Anti-Exploit are trademarks of Malwarebytes Corporation. Windows, Windows 8, Windows 7, Windows Vista and Windows XP are registered trademarks of Microsoft Corporation. All other trademarks or registered trademarks listed belong to their respective owners.

Copyright © 2014 Malwarebytes Corporation. All rights reserved.

# Contents

---

<b>Notices</b> .....	<b>2</b>
<b>1.0 System Requirements</b> .....	<b>5</b>
<b>2.0 Installation</b> .....	<b>7</b>
2.1 Retail CD .....	7
2.2 Program Download .....	7
2.3 Common Installation.....	7
2.4 A Final Word About Administrative Rights.....	8
2.5 Activation.....	8
<b>3.0 Screen Layout</b> .....	<b>11</b>
3.1 Menu Bar .....	11
3.2 Main Window .....	11
<b>4.0 Dashboard</b> .....	<b>13</b>
4.1 Status Banner .....	13
4.2 License .....	14
4.3 Database Version .....	14
4.4 Scan Progress .....	14
4.5 Real-Time Protection .....	14
4.6 View License Details .....	14
4.6.1 Deactivate .....	15
4.6.2 Change License.....	15
<b>5.0 Scan</b> .....	<b>17</b>
5.1 Threat Scan .....	17
5.2 Custom Scan .....	17
5.3 Hyper Scan.....	19
5.4 Scan Results .....	19
5.5 View Detailed Log.....	19
<b>6.0 Settings</b> .....	<b>23</b>
6.1 General Settings .....	24
6.1.1 Notifications.....	24
6.1.2 Close Notification.....	24
6.1.3 Language.....	24
6.1.4 Explorer context menu entry.....	24
6.2 Malware Exclusions.....	25
6.2.1 Add File .....	25
6.2.2 Add Folder .....	26
6.2.3 Remove .....	26
6.3 Web Exclusions .....	26
6.3.1 Add IP .....	27

6.3.2	Add Domain.....	27
6.3.3	Add Process .....	27
6.3.4	Remove .....	28
6.4	Detection and Protection.....	28
6.4.1	Detection Options .....	28
6.4.2	Non-Malware Protection.....	28
6.4.3	Malware Protection (Premium/Trial versions only) .....	29
6.4.4	Malicious Website Protection (Premium/Trial versions only) .....	29
6.5	Update Settings .....	29
6.5.1	Update Options .....	30
6.5.2	Proxy Settings .....	30
6.6	History Settings.....	31
6.6.1	Statistical Data .....	31
6.6.2	Scan Log Options.....	31
6.7	Access Policies.....	32
6.8	Advanced Settings .....	34
6.9	Automated Scheduling.....	35
6.9.1	Basic Mode .....	35
6.9.2	Advanced Mode .....	37
6.9.3	Advanced Scan Options.....	37
6.9.4	Advanced Update Check Options.....	38
6.10	About.....	38
<b>7.0</b>	<b>History .....</b>	<b>39</b>
7.1	Quarantine .....	39
7.2	Application Logs.....	39
7.2.1	Protection Log.....	40
7.2.2	Scan Log .....	41
7.2.3	Viewing or Deleting Logs.....	41
	<b>Appendix A: Notification Window Examples .....</b>	<b>43</b>

## 1.0 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 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**

This page left intentionally blank

## 2.0 Installation

---

Malwarebytes Anti-Malware is available in two forms, retail CD and download. Most aspects of the installation are identical, though there are some differences due to different media being involved.

### 2.1 Retail CD

---

Insert the Malwarebytes CD into your CD/DVD player, and close the door. The Malwarebytes installer should begin automatically. If it does not begin automatically, do the following:

- Open Windows Explorer
- Navigate to your CD/DVD drive
- Go to the **Tools** directory
- Double click on file **mbam-setup-2.0.1.xxx.exe** to launch the installation program. **xxx** represents the specific build of the program, and will change depending on exactly when you downloaded the program. **Please note** that the ".exe" portion of the filename may not be visible if you do not have Windows Explorer configured to show file extensions.

The remainder of the installation process for the Retail CD version of Malwarebytes Anti-Malware can be found just below in the *Common Installation* section.

### 2.2 Program Download

---

To begin the installation, double-click on the Malwarebytes Anti-Malware installation file which you downloaded.

### 2.3 Common Installation

---

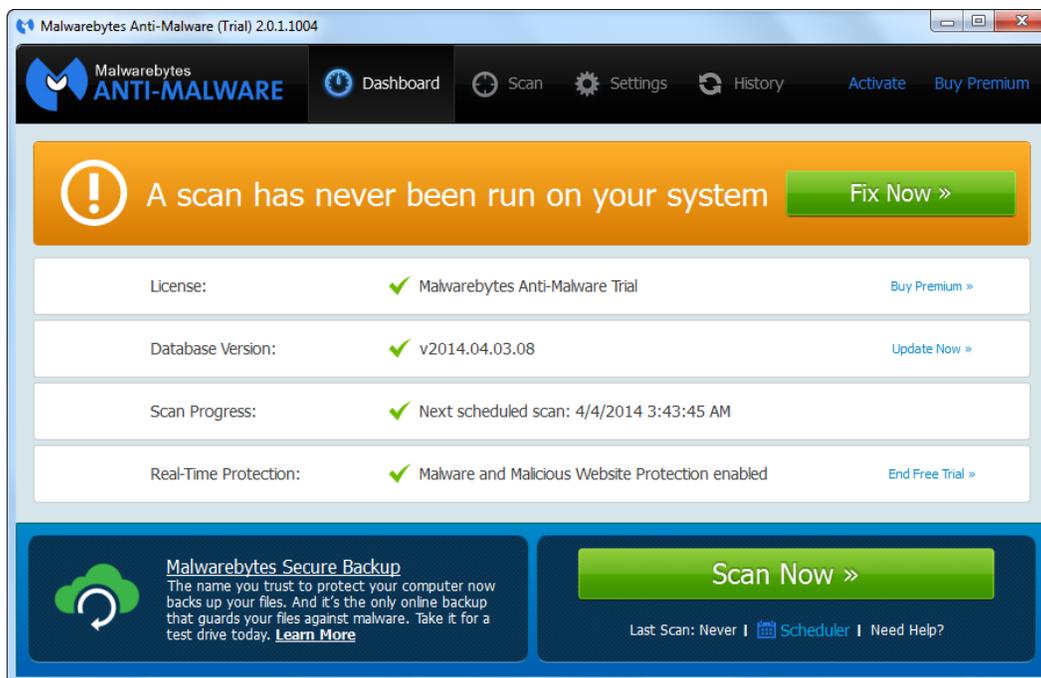
If you are installing Malwarebytes Anti-Malware on a Windows version newer than Windows XP, a Windows dialog box will be presented in the middle of your screen, labeled **User Account Control**. Verify that the publisher is listed as [Malwarebytes Corporation](#) and click **Yes**. This is a Windows security feature that began with Windows Vista to assure that an application's capabilities are limited unless and until you authorize higher capabilities. Once approved, the 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 choose to enable a free trial of Malwarebytes Anti-Malware Premium, and you may also 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 in the black Menu Bar at the top of the Malwarebytes user interface.

You will notice the orange banner across the interface which tells you that a scan has not been run on this computer. Click the **Fix Now** button to run your first scan.



As the scan began, you likely noticed messages in the lower right corner of your screen that came and went. These are Malwarebytes *notifications* which inform you of changes, updates, and items which require your immediate attention. You can see all of the notifications which appear during operation of Malwarebytes Anti-Malware in Appendix A of this guide.

## 2.4 A Final Word about Administrative Rights

---

If you installed Malwarebytes Anti-Malware from a downloaded installation file, you had the option of starting a free trial of our Premium version, as well as the capability to activate the Premium features if you had purchased an annual subscription. You may have decided to wait until later. If that is the case, please remember that you should be logged in to Windows as an *Administrator* before doing either of those tasks.

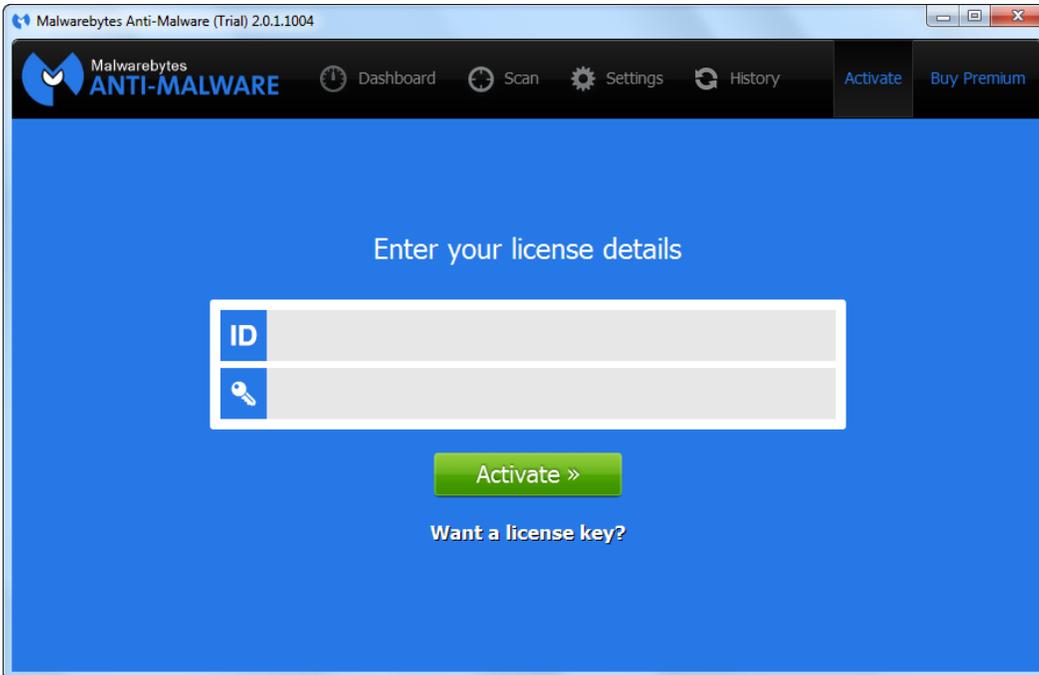
## 2.5 Activation

---

Malwarebytes Anti-Malware is available for any Windows user to download and install at no cost to them. They can also purchase an annual subscription, which entitles them to take advantage of real-time protection, scan/update scheduling, access policies, and the ability to utilize all of these features on up to three computers under the same license.

If no license has been installed into the product, the black Menu Bar at the top of the screen will show two links titled **Activate** and **Buy Premium**. When clicked, **Buy Premium** takes the user to a screen which shows the advantages of purchasing a license, and provides the option of launching a browser window which will take them to the Malwarebytes web site to purchase a license.

If the user has already purchased a license, and wishes to activate the product, clicking the **Activate** link shows the following screen...



Your license information will be either in the form of a sticker which was enclosed with your retail Malwarebytes CD, or in an email sent to you by Malwarebytes at the time of purchase. Locate the license information, enter both the **ID** and **Key**, then click the **Activate** button. Your Malwarebytes screen will refresh, as shown below.



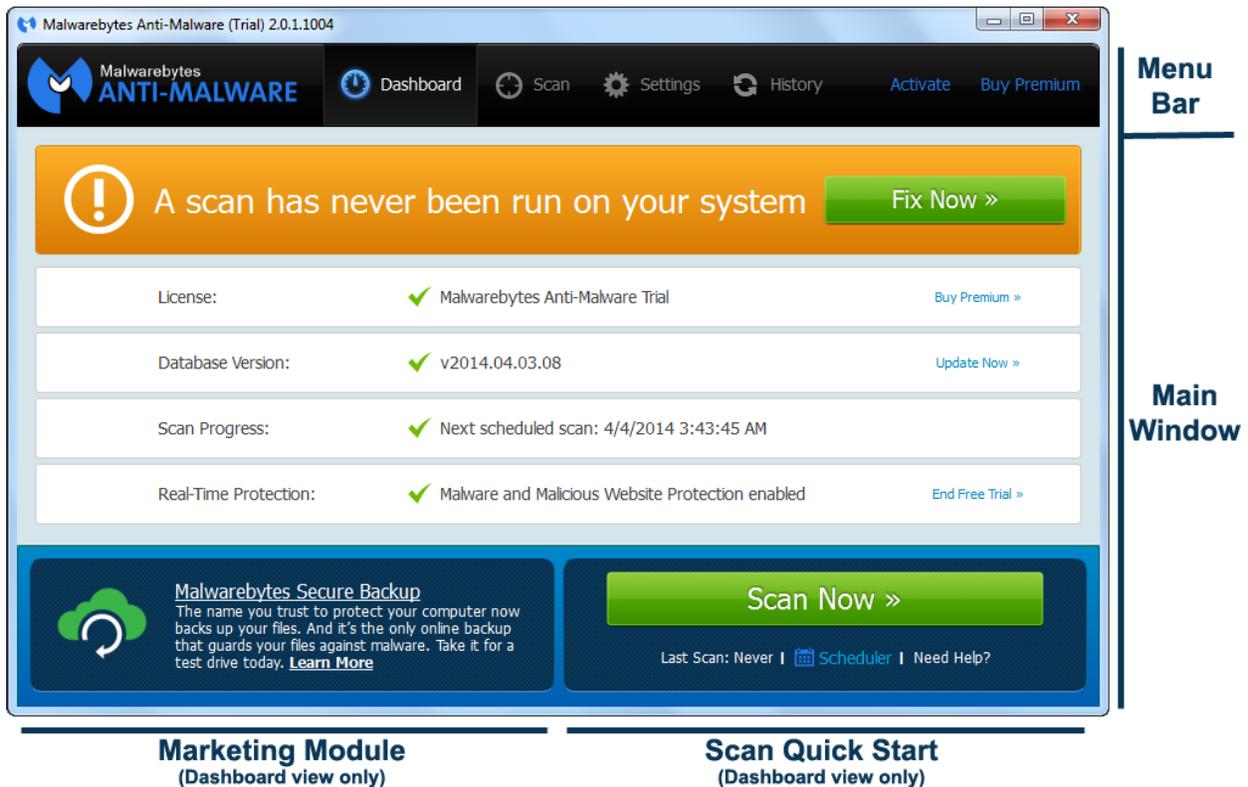
Please note that the two license-related links in the Menu Bar have been replaced by a link called **My Account**. Also note that the License has changed from *Malwarebytes Anti-Malware Trial* to *Malwarebytes Anti-Malware Premium*.

We will go into much more detail about the features of Malwarebytes Anti-Malware, but before doing that, we should introduce you to the Malwarebytes user interface.

This page left intentionally blank

## 3.0 Screen Layout

The Malwarebytes Anti-Malware program interface is designed around a screen layout which is simplified and uncluttered. We want to make it easy for you to configure the program to serve your needs, and we hope this layout helps to do that. The screenshot below shows the Malwarebytes user interface, showing the Dashboard – the first screen you see when Malwarebytes Anti-Malware is launched for the first time.



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

### 3.1 Menu Bar

The Menu Bar contains the main program options, which will be discussed in detail in this guide. They consist of:

- **Dashboard:** What you see here. While the exact details change over time, the look is consistent.
- **Scan:** Select the type of scan you wish to run, run it, and view the results.
- **Settings:** Configure every aspect of Malwarebytes Anti-Malware, so that it can protect you efficiently.
- **History:** View historical logs containing information on program updates, database updates, and scan results.

In addition, there are settings for Account information. While in free trial mode, options are present to **Activate** the program, or to buy the premium subscription. Once you have purchased a subscription, those two options will revert to a single option which handles details of your account. More on those later.

### 3.2 Main Window

This is the area where almost all activities related to configuration and operation of Malwarebytes Anti-Malware will be displayed. In Dashboard mode, there are two smaller sub-panels which appear at the bottom of the Main Window. The *Marketing Module* displays messages to inform you of products and services that we have to offer. The *Scan Quick*

*Start* allows you to initiate a scan based on current configuration settings. You will find that while our pre-defined settings will work well for you, your own settings can fine-tune your results.

In all other modes, the Main Window is subdivided in a different manner. The left edge of the screen is reserved for a column of buttons (or tabs if you prefer). Clicking any button launches appropriate program content in the remainder of the Main Window. More on this later.

In the meantime, let's continue by looking at the *Dashboard* in more detail.

## 4.0 Dashboard

Each time Malwarebytes Anti-Malware is launched, the first page visible to the user is the *Dashboard*. It is designed to provide Malwarebytes status, and to act as a *launch pad* for all program operations. A screenshot of the user interface – featuring the Dashboard – is shown below for reference.



### 4.1 Status Banner

Within the Main Window, the first item displayed is the Status Banner. This banner displays a status message determined by the program on a color-coded background. This background is meant to alert the user to conditions which may require intervention. Colors are used which are similar to traffic stop signals – *green* simply indicates a good status; *orange* indicates a warning of a condition which may become more severe over time; *red* indicates that your immediate attention is needed. Following is a full list of status messages. If a recommended method of correcting the problem is immediately available, it will appear as a functional button on the banner itself.

- **Color: green (no problem)**
  - Your system is fully protected
  - Malwarebytes Anti-Malware (Free)
- **Color: orange (non-critical problem)**
  - A scan has never been run on your system
  - Your databases are out of date
  - Your program version is out of date
  - Your trial will expire in <X> days
  - Your License will expire in <X> days
- **Color: red (critical problem)**
  - Your free trial has expired
  - Your License period has expired
  - Your system is not fully protected

## 4.2 License

---

If you have purchased a license for your copy of Malwarebytes Anti-Malware, it is shown here. If your license type is *Malwarebytes Anti-Malware Premium*, there is a [View Details](#) link available which allows you to access two options related to your license. That will be covered a bit further down in this section. If you have not purchased a license, the license will be listed as *Malwarebytes Anti-Malware Trial*. There will also be a [Buy Premium](#) link, which you may click if you wish to purchase a subscription to the Premium features.

## 4.3 Database Version

---

This item shows the version of the Malwarebytes Rules database which is currently installed. Referring to the screenshot (above), the database version is shown as v2014.04.03.08. The version number indicates that the database was created on April 3, 2014, and was the eighth update released on that day. Dates incorporated into the version number are referenced to Greenwich Mean Time (GMT). This means that versions could appear to be *in the future* depending on the difference between GMT and your time zone. That could change on an hour-by-hour basis. That said, your biggest concern here is a version number that is clearly in the past. Because there is a green checkmark to the left of the version number, that indicates that this screenshot was created while at a time that the database was considered current.

Clicking the **Update Now** link causes Malwarebytes Anti-Malware to attempt a non-scheduled database update. If an update is available, you will see a progress bar which shows status of the update until the update has completed. The Database Version will then show a new version number. If no updates are available, the progress bar will indicate the update attempt, to be replaced by the text "No updates available" for several seconds. The database version number will again be displayed.

**Please note** that database updates only occur automatically if you are using Malwarebytes Anti-Malware on a free trial, or if you are a licensed (Premium) user. If you are using the free version, you must manually update the database.

## 4.4 Scan Progress

---

This item shows when the next scan is scheduled to occur. Clicking the **Scan Now** button will cause a scan to occur immediately, and change to the [Scan](#) screen at the same time. Clicking the **Dashboard** button at that time will allow you to see scan progress reflected on the Dashboard, though the [Scan](#) screen provides much more detailed information. **Please note** that scheduled scans are available only if you are using Malwarebytes Anti-Malware on a free trial, or if you are a licensed (Premium) user. This feature is not available if you are using the free version.

## 4.5 Real-Time Protection

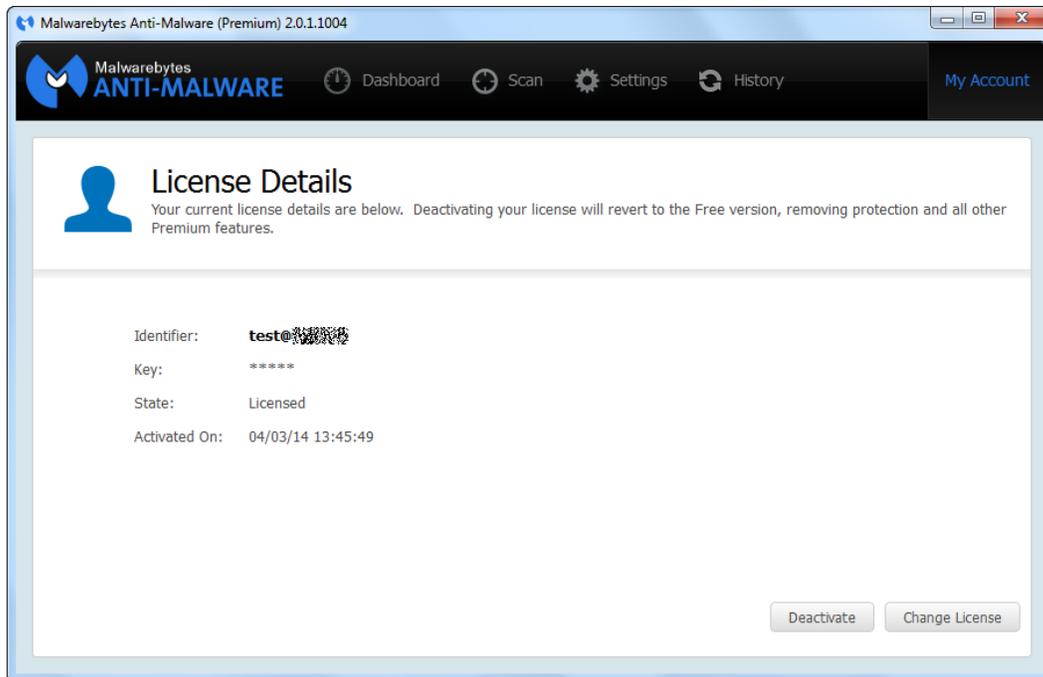
---

This item shows whether Real-Time Protection is enabled or disabled. If you are in free trial mode, it is enabled unless you click the **End Free Trial** button. **Please note** that real-time protection is enabled only if you are using Malwarebytes Anti-Malware on a free trial, or if you are a licensed (Premium) user. This feature is not available if you are using the free version.

## 4.6 View License Details

---

If you have purchased an annual subscription for premium services, this page is accessible from the [Dashboard](#) via the **View Details** link. A screenshot of the page is shown below.



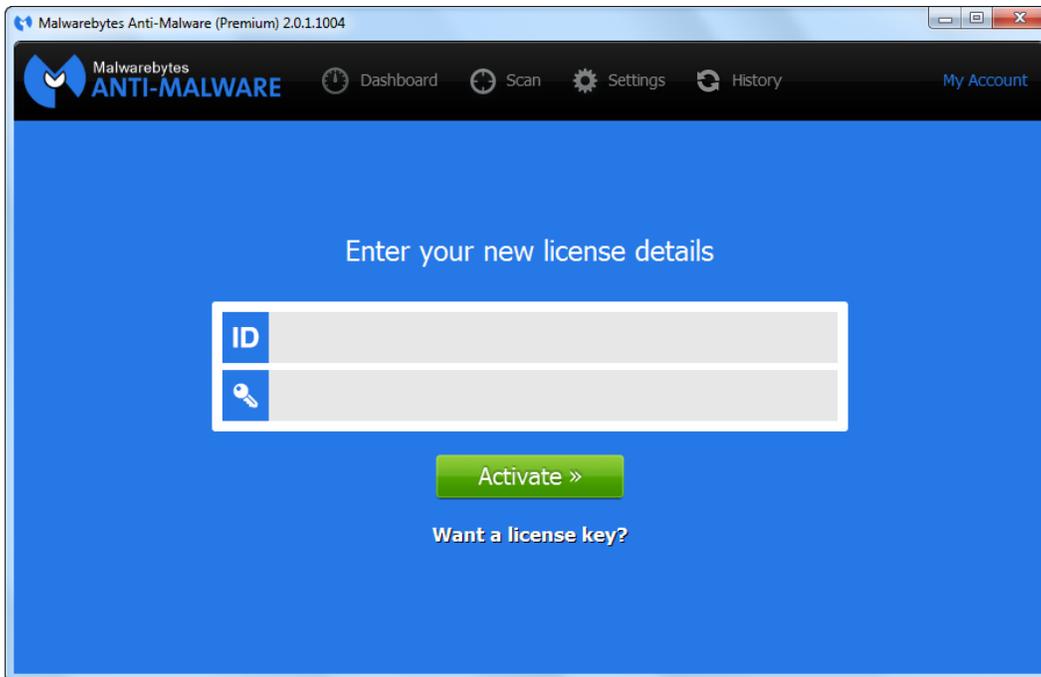
This page shows the email address or ID (Identifier) used during product activation, the license state, and the date the license was activated. If you require technical support or license support, information from this page will be requested from you. In addition to this information, there are links in the bottom right corner which allow you to **Deactivate** or **Change License**.

#### 4.6.1 Deactivate

Clicking this link brings up a prompt asking you to confirm that you want to deactivate your license. This is a method you could use as part of transferring your Malwarebytes subscription to another computer.

#### 4.6.2 Change License

Clicking this link brings up a screen so that you can enter a new ID and Key to replace those that are currently in use. This screen is shown here.

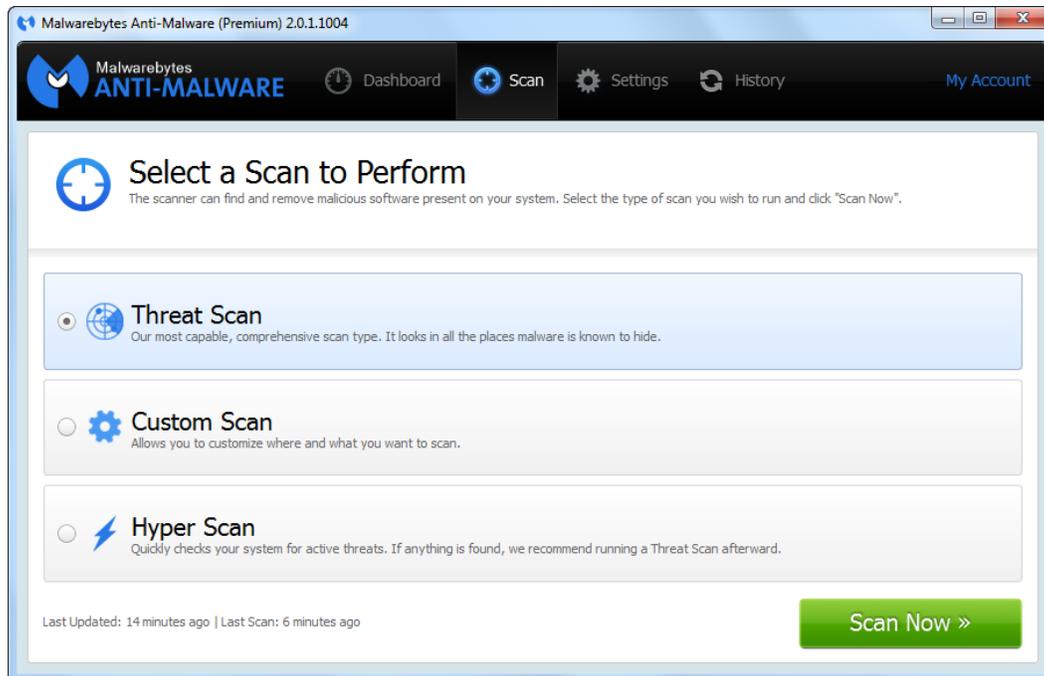


This would be a preferred method if you received a new product license.

## 5.0 Scan

---

The Scan option is available from the Malwarebytes Menu Bar. There are two screens directly associated with this option. The screen shown below is your initial view into this option.



Once you have executed a scan, the program refers to this screen as the Main Menu. Don't be confused by the name...it is a menu in the sense that you may choose a type of scan to execute from this screen, but it is not a main menu for Malwarebytes as a whole.

This page does not allow you to make configuration changes for scans. These are made on the *Settings* page, to be discussed in Section 6. There are three types of scans which can be selected and executed here. Let's talk about each...

### 5.1 Threat Scan

---

This method of scanning detects a large majority of threats that your computer may be faced with. Areas and methods tested include:

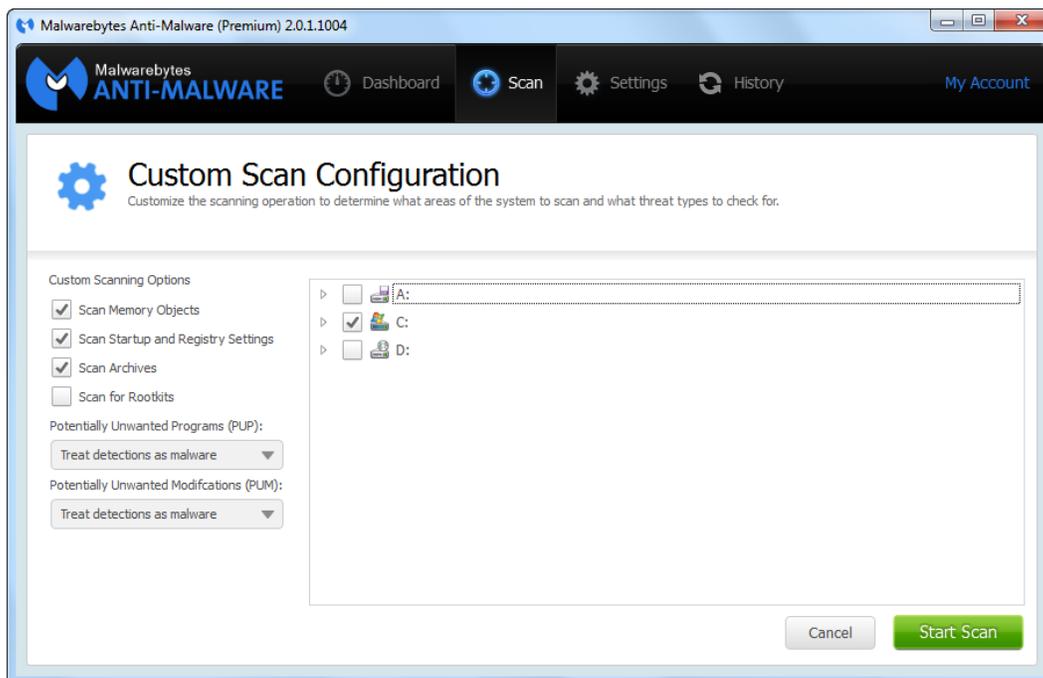
- **Memory Objects:** Memory which has been allocated by operating system processes, drivers, and other applications.
- **Startup Objects:** Executable files and/or modifications which will be initiated at computer startup.
- **Registry Objects:** Configuration changes which may have been made to the Windows registry.
- **Filesystem Objects:** Files stored on your computer's local disk drives which may contain malicious programs or code snippets.
- **Heuristic Analysis:** Analysis methods which we employ in the previously-mentioned objects – as well as in other areas – which are instrumental in detection of and protection against threats, as well as the ability to assure that the threats cannot reassemble themselves.

### 5.2 Custom Scan

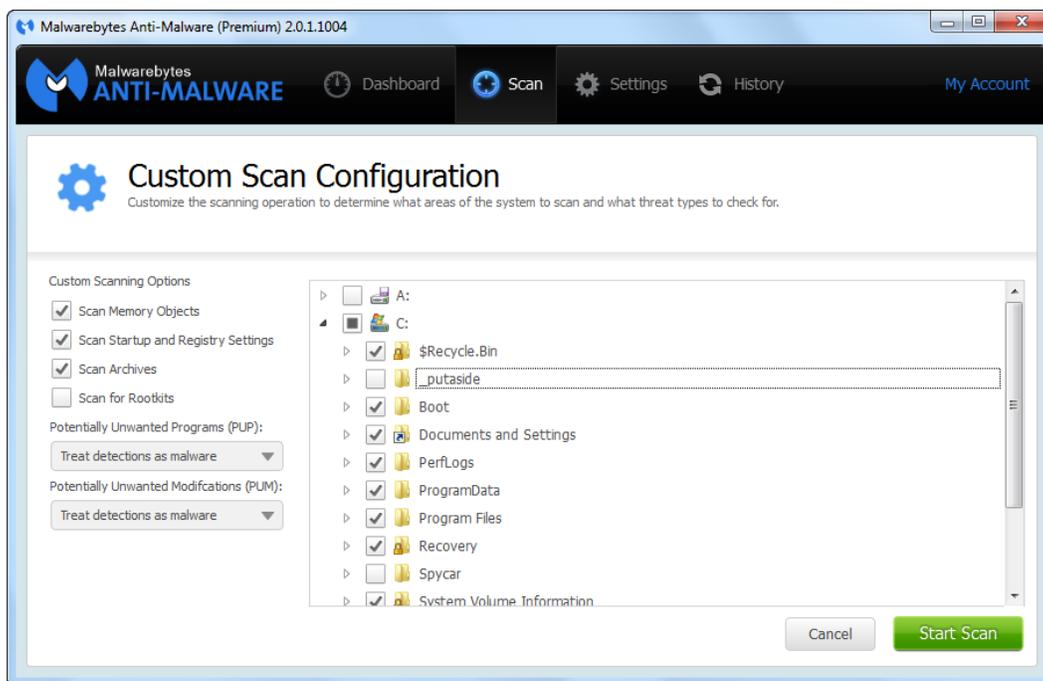
---

You may also choose to run a custom scan. A custom scan allows you to scan according to specifications which you define at the time of the scan. All other Malwarebytes scans are performed according to a set of specifications which

you define in *Settings* (to be discussed in Section 6). Here, you can run a "one-off" if you wish. A screenshot of the custom scan configuration screen is shown below.



Custom scanning options (left side of the screen) have been discussed somewhat in the text above, and are discussed much more fully in *Settings*, to be discussed in Section 6. An important feature to note here is the ability to specify certain areas of your file system for scanning, using a Windows Explorer-like presentation model. In the screenshot below, two specific directories have been excluded from scanning by unchecking them.



You will notice that the checkbox for OS (C:) is now filled by a square instead of a checkbox. This indicates that *some* of this drive (but not all) will be scanned. You may have your own reasons why certain directories should be scanned or ignored, but Malwarebytes Anti-Malware gives you the ability to make that choice.

## 5.3 Hyper Scan

---

This scanning option is only available to users of Malwarebytes Anti-Malware Premium and Trial versions. This method of scanning is limited to detection of immediate threats. Areas and methods tested include:

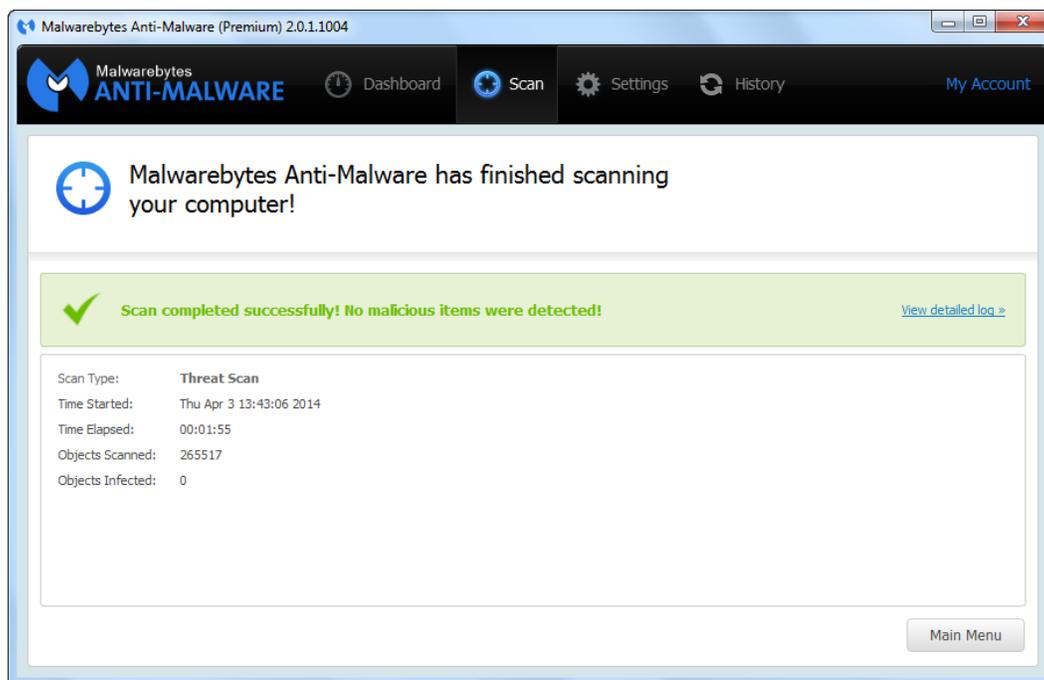
- **Memory Objects:** Memory which has been allocated by operating system processes, drivers, and other applications.
- **Startup Objects:** Executable files and/or modifications which will be initiated at computer startup.
- **Heuristic Analysis:** Analysis methods which we employ in the previously-mentioned objects – as well as in other areas – which are instrumental in detection of and protection against threats, as well as the ability to assure that the threats cannot reassemble themselves.

While a Hyper Scan will clean any threats which have been detected, we strongly recommend that a [Threat Scan](#) be performed if a Hyper Scan has detected threats.

## 5.4 Scan Results

---

After a scan has been executed, a different page appears, as shown below.

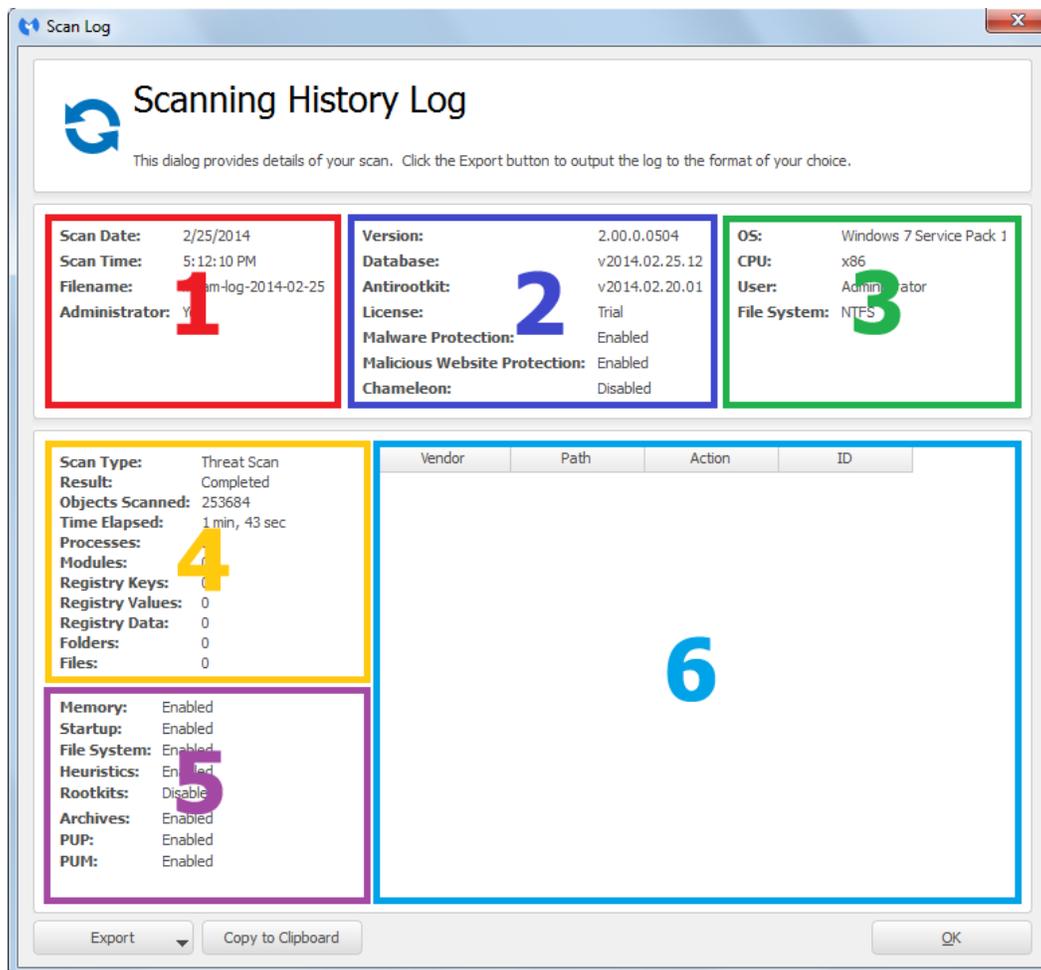


In this case, a green status bar shows scan results. The color by itself indicates that no problems were detected, however the message should always be read in case any user actions are required. Basic details about the scan are displayed here as well. There is a link at the right side of the status bar which allows us to *View Detailed Log* results. There is also a button at the bottom which allows you to return to the *Main Menu* should you wish to run another scan.

## 5.5 View Detailed Log

---

Each time a scan is executed, a log is created. The *Scan* screen provides a one-line summary in the Status bar. The Status bar also contains a *View Detailed Log* link, which allows you to study scan results in detail. That log is saved in either extensible markup language (XML) or plain text format (TXT), as configured in *History Settings* (Section 6.6). A sample log (in XML format) is shown here.



Information is presented in six boxes, so that it is organized into groups. Following is a listing of log contents. Designation of each data group is superimposed over the screenshot.

- Group 1 (top left) – **Scan Information**
  - **Scan Date:** Date when scan was executed
  - **Scan Time:** Time when scan was completed
  - **Filename:** Log file name, which includes year, month, day, hour, minute, and second in the filename. Times use a 24-hour clock, and are referenced to the start time of the scan.
  - **Administrator:** Whether the user running the scan was logged on with administrator rights
- Group 2 (top center) – **Version Information**
  - **Version:** Malwarebytes Anti-Malware program version
  - **Database:** Malwarebytes rules database version
  - **Antirootkit:** Malwarebytes Anti-Rootkit version
  - **License:** License type (valid values are Free, Premium or Trial)
  - **Malware Protection:** Whether malware protection is enabled (valid values are enabled or disabled)
  - **Malicious Website Protection:** Whether malicious website protection is enabled (valid values are enabled or disabled)
  - **Chameleon:** Whether *Chameleon* self-protection is enabled (valid values are enabled or disabled)
- Group 3 (top right) – **Computer Version Information**
  - **OS:** Operating System version, which also may contain Service Pack information
  - **CPU:** CPU type (valid values are x86 and x64)
  - **User:** Windows user name associated with this scan

- **File System:** File system used on the primary (OS) disk drive (valid values are NTFS, FAT and FAT32)
- Group 4 (center left) – **Scan Details**
  - **Scan Type:** Type of scan executed (valid values are Threat Scan, Custom Scan, Hyper Scan and Context Scan)
  - **Result:** Final scan result (valid values are cancelled, completed or failed)
  - **Objects Scanned:** Number of objects scanned
  - **Time Elapsed:** Elapsed time of scan, from start to finish
  - **Remaining Categories:** For each category, the number of items detected during the scan
- Group 5 (bottom left) – **Object Types/Targets Scanned**
  - Eight object types/targets are listed. Each may be enabled (included in scan) or disabled (excluded from scan)
- Group 6 (bottom right) – **Detected Threats**
  - Threats detected during scan execution, containing the following information:
    - **Vendor:** Name of threat, threat family, or threat type (as categorized by Malwarebytes Research team)
    - **Path:** Location where the threat was found; This will be a directory/file name for file system-based threats, and key/value name/value data for registry-based threats
    - **Action:** What action was taken with regard to the detected threat
    - **ID:** This is the identifier that Malwarebytes Research team uses for the specific threat. This may be requested by Malwarebytes Technical Support if a question arises pertaining to blocking of a specific threat.

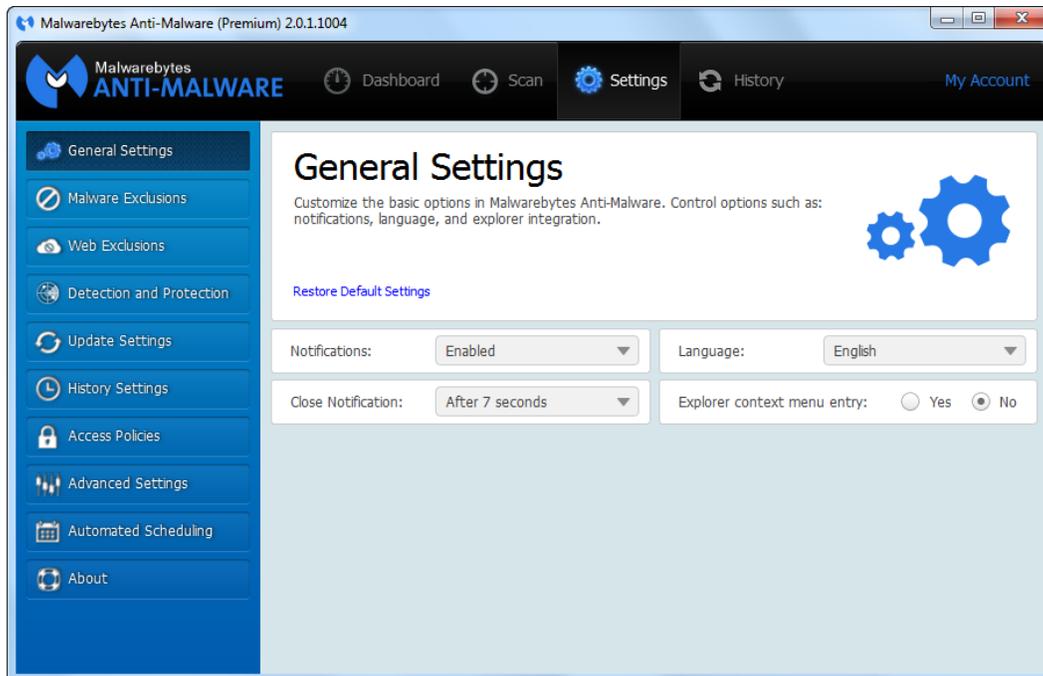
At the very bottom of the [Scan Log](#) are two buttons, **Export** and **Copy to Clipboard**. Clicking the **Export** button will allow the log to be exported into Extensible Markup Language (XML) or text (TXT) file. **Copy to Clipboard** allows the log to be copied into your Windows clipboard. In this format, each item of information is presented on a line-by-line basis, with no formatting added.

If you have configured your *History Settings* (Section 6.6) to provide logs in text (TXT) format, logs will be identical to those produced by copying an XML log to your Windows clipboard.

This page left intentionally blank

## 6.0 Settings

The [Settings](#) screen is the top-level page which controls all configuration settings for Malwarebytes Anti-Malware. A screenshot of this screen is shown below.



Throughout this section, the Main Window is divided into two areas. The left edge shows a column of blue buttons. We have grouped settings by the areas/functions which they control, in order to maintain a clean user interface. These buttons provide access to each of the various groups of settings. As you click any of the buttons, you will see the large portion of the Main Window change to reflect the button which you pushed. At the same time, the background of the button itself changes color. Also, if you navigate away from *Settings* – to *Dashboard*, *Scan* or *History* – you will always return to the [General Settings](#) tab when you click on [Settings](#).

Before we dig in to each of the Settings tabs, a brief description of each is in order.

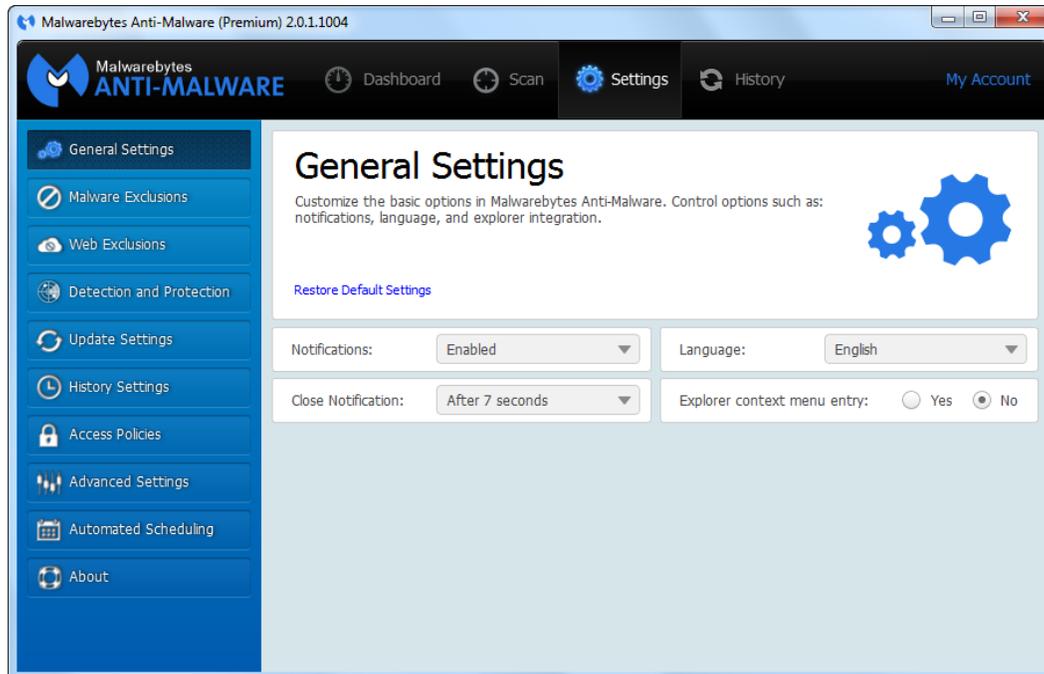
- **General Settings:** Look and feel of Malwarebytes Anti-Malware
- **Malware Exclusions:** Files and/or folders to be excluded from scanning
- **Web Exclusions:** IP addresses, internet domains or processes to be excluded from blocking by Malwarebytes Website Protection
- **Detection Settings:** Behavior of Malwarebytes Anti-Malware as it relates to threat detection
- **Update Settings:** Settings related to program or rules database updates
- **History Settings:** Formatting of program logs
- **Access Policies:** "Who can do what." This is of value when multiple people use the same computer.
- **Advanced Settings:** Specific behavior of real-time protection
- **Automated Scheduling:** Scheduling of scans and updates
- **About:** Program version number

Most Settings tabs offer a link (in the upper section of the Main Window) to return settings to their original state. For each tab, this guide will specify the default/recommended value for each setting.

Now, let's take a look at *General Settings*!

## 6.1 General Settings

This is the first screen you will see when you click on [Settings](#) in the Menu Bar. It controls the basic look and feel of Malwarebytes Anti-Malware. A screenshot of this screen is shown below.



There are four settings which can be configured here. They are as follows:

### 6.1.1 Notifications

Notifications regarding rules database updates, program updates, and scan operations occur in notification windows. These windows appear at the lower right corner of your screen, outside of the Malwarebytes Anti-Malware interface. You may enable or disable these notifications. Notifications are enabled by default. **Please note** that some non-critical information may not be visible if you disable notifications.

### 6.1.2 Close Notification

When a notification window is displayed on your screen, it remains visible for a time period which you configure here. That time is configurable in a range of 3-15 seconds. The default time is 7 seconds.

### 6.1.3 Language

This setting determines the language used throughout the Malwarebytes Anti-Malware program. This is pre-set, based on the language used during program installation. It can be modified at will.

### 6.1.4 Explorer context menu entry

Malwarebytes Anti-Malware has the capability to launch a *Threat Scan* upon one or more individual files or directories from within Windows Explorer by using the context menu that becomes available when the files/directories are right-clicked. This setting allows that capability to be turned on or off. The default setting is Yes (on).

## 6.2 Malware Exclusions

This screen allows you to exclude files and/or folders from scans executed by Malwarebytes. While you may have your own reasons for excluding files or folders from scans, the primary reason for doing so is to prevent potential conflicts with anti-virus software. Malwarebytes works well alongside most anti-virus software, but anti-virus updates by some

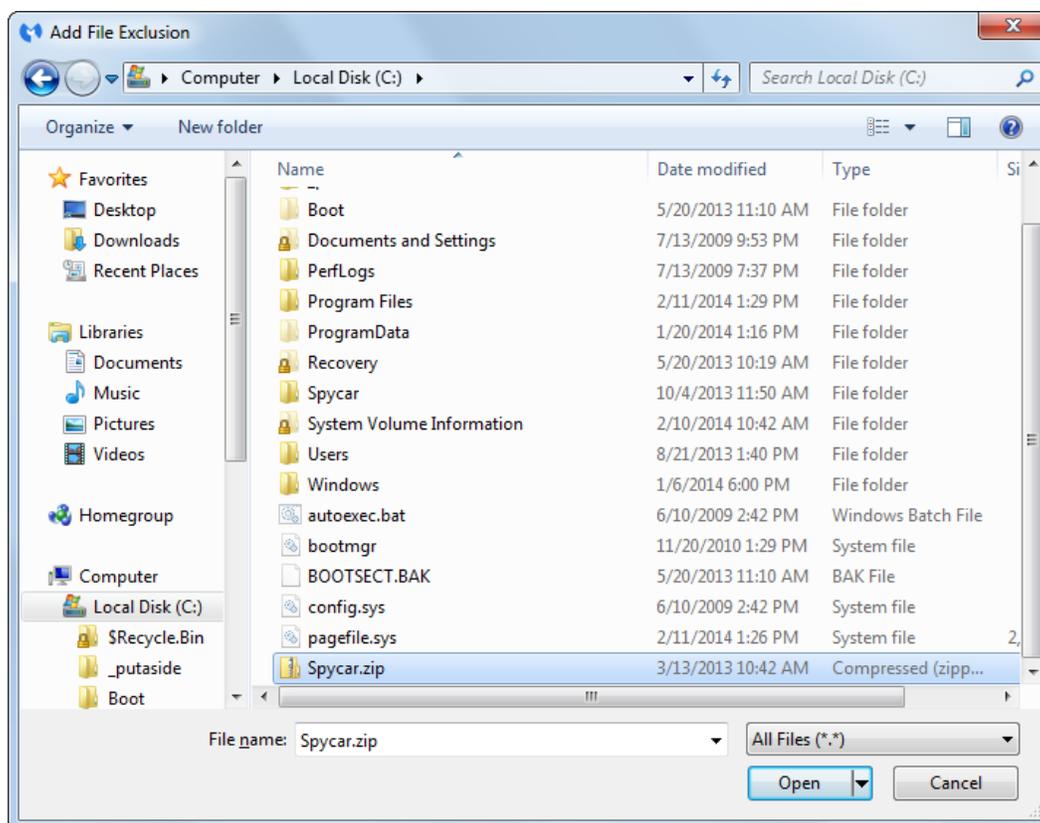
vendors may occasionally be flagged as a threat. For this reason, we offer the provision for you to exclude certain disk content from scanning. This provision is commonly offered by anti-virus vendors as well. A screenshot of this screen is shown below.



This screen features three actions which may be performed. The bottom half of the Main Window shows results of these actions.

### 6.2.1 Add File

Clicking the [Add File](#) button allows you to exclude one file from scanning by Malwarebytes Anti-Malware. The file to be excluded is selected in a separate window, which is shown here.



If you wish to exclude multiple files within a single directory, you must exclude each individually. You may exclude as many files as you wish, but they must be specified individually. Once specified, the file will appear in the Exclusion List in the main window. **Please note** that the dimensions of this window have been modified from the size that the window opens to initially. This was done for clarity of presentation here. You may modify the size of this window to suit your needs as well.

## 6.2.2 Add Folder

You may also exclude folders from scanning. As with files, you may exclude as many folders as you wish, but each must be specified individually. **Please note** that selecting a folder for exclusion will also cause every file in that folder as well as any sub-folders and files contained within those sub-folders to be excluded. Folder exclusion will be performed in a second window which is identical in construction to the window used for file exclusion. Once selected, excluded folders will be shown in the exclusion List.

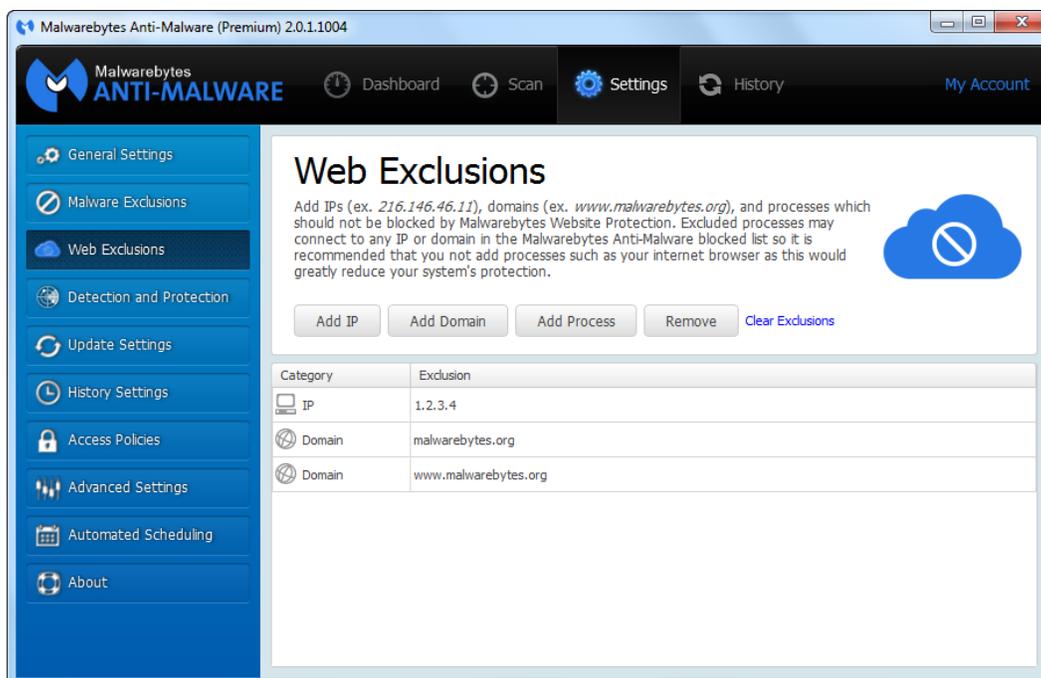
## 6.2.3 Remove

It is a very simple process to remove a file or folder from the Exclusion List. Click on the file or folder in the Exclusion List, then click the **Remove** button. It will immediately disappear from the Exclusion List, and will no longer be excluded.

## 6.3 Web Exclusions

This screen allows users of Malwarebytes Anti-Malware Premium and Trial versions to exclude IP addresses, Internet domains and processes from Website Protection. This screen is disabled for users of the free version, because Malicious Website Protection is disabled in the free version.

**Please note** that this is not a method of blocking access. It is exactly the opposite. Unless you are a knowledgeable computer user, you will likely find out what needs to be excluded because of blocked access to a web site and resulting notifications that alerted you to the block. A screenshot of this screen is shown here.



For demonstration purposes, three entries have been added to the Web Exclusion list shown on this screenshot. These are described here.

### 6.3.1 Add IP

Clicking the **Add IP** button allows you to exclude an IP address from Malwarebytes Website Protection. You should not use wildcard characters in the IP address to be executed, as exclusions of IP addresses which you are not familiar with can compromise your safety. You can also add an IP address exclusion when it is blocked by Malwarebytes Website Protection by clicking the link in the block notification message.

### 6.3.2 Add Domain

Clicking the **Add Domain** button allows you to exclude an internet domain from Malwarebytes Website Protection. You can also add an internet domain exclusion when it is blocked by Malwarebytes Website Protection by clicking the link in the block notification message. **Please note** the following two important items:

- If adding a domain manually, you should add it both with and without the "www." prefix. Depending on several external factors, the domain may still be blocked if only one variation is entered.
- The ability to add a domain to the Web Exclusion list is only functional on Windows Vista Service Pack 2, Windows 7, and Windows 8.x.

### 6.3.3 Add Process

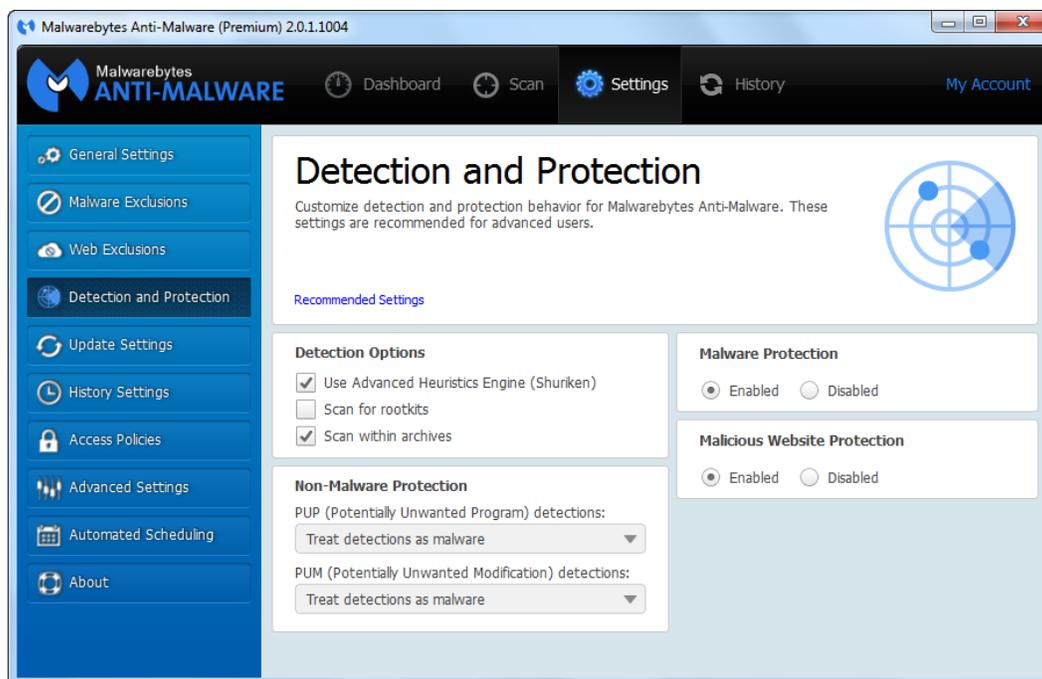
Clicking the **Add Process** button allows you to exclude a process which would otherwise be blocked from accessing an internet address. **Please note** that this option is only functional on Windows Vista Service Pack 2, Windows 7, and Windows 8.x. This is typically of value to users who need to access file sharing and/or peer-to-peer applications. On occasion, IP addresses used by these applications may be blacklisted, so that Malwarebytes Website Protection blocks access to the website as a whole. Excluding the IP address makes the user more vulnerable, as would exclusion of the domain (if the website uses a domain name). Excluding the process – providing that the process is not an internet browser – would allow the P2P application to function without increasing risk.

### 6.3.4 Remove

It is a very simple process to remove an IP address, domain or process from the Exclusion List. Click on its entry in the Exclusion List, then click the **Remove** button. It will immediately disappear from the Exclusion List, and will no longer be excluded.

## 6.4 Detection and Protection

This screen allows you to define how Malwarebytes Anti-Malware searches for potential threats on your computer, and what actions will be taken when threats are detected. A screenshot of this module is shown below, with recommended (default) settings displayed.



### 6.4.1 Detection Options

The Detection Options settings determine specifically what methods Malwarebytes Anti-Malware uses to detect and identify modifications which are determined (or suspected) to be malicious in nature. **Use Advanced Heuristics Engine (Shuriken)** enables a second method of heuristic analysis to our malware detection techniques. Heuristic analysis is always employed, even when this option is not selected.

**Scan for rootkits** utilizes a specific set of rules and tests to determine if a rootkit is present on your computer. For readers who unfamiliar with this term, an explanation may be handy. A rootkit is malicious software that can be placed on a computer which can modify operating system files in a manner that hides its presence. Malware detection methods that rely on hooks to the operating system for detection and analysis would prove ineffective if the hooks had been purposely manipulated by the malware. Our testing method is more intensive and more effective, but including rootkit scans as part of your overall scan strategy increases the time required to perform a scan.

When **Scan within archives** is enabled, Malwarebytes Anti-Malware will scan three levels deep within archive (ZIP, RAR, 7Z, CAB and MSI) files. If this option is disabled, only the first level of the archive is tested. **Please note** that encrypted archives cannot be fully tested.

### 6.4.2 Non-Malware Protection

In addition to malicious software detection and elimination, Malwarebytes Anti-Malware also detects and acts upon two classes of *non-malware*. These are Potentially Unwanted Programs (PUP's) and Potentially Unwanted

Modifications (PUM's). In many cases, PUP's appear in the form of toolbars and other application software which are installed on your computer as part of a bundle. You may have asked for one application, and it came with a second application that was not mentioned, *or* was mentioned, but you did not uncheck the checkbox next to it to prevent it from being installed at the same time. You may also want and use the PUP. We do not judge the merit of the program or its usability. We do offer a method of removing it if you choose to.

PUM's are a bit different. These are modifications that are typically related to the Windows registry. As a user, you will generally not be making changes to the registry that would qualify as a PUM – though the possibility does exist. Because it does, we allow you to define your own rules when it comes to how they are treated.

With regard to both types of modifications, we provide three handling methods within Malwarebytes Anti-Malware. These are:

- **Ignore Detections:** Malwarebytes will not act on detection, nor will you be alerted.
- **Warn user about detections:** You will be alerted to the detection, and you may choose to ignore it, create an exclusion, or treat it as malware.
- **Treat detections as malware:** The detection will be treated as malware, and corrective actions will occur.

While PUP's and PUM's are both handled in the same manner, each is handled according to separate guidelines which you specify.

### **6.4.3 Malware Protection (Premium/Trial versions only)**

Malwarebytes Anti-Malware allows you to disable Malware Protection when necessary. While we do not recommend disabling this protection mechanism, there may be times when it needs to be done to troubleshoot issues that arise with compatibility issues with anti-virus updates or computer startup problems. If either situation does occur, start your computer in Safe Mode, disable Malwarebytes Malware Protection, isolate and correct the issue, then turn Malware Protection back on. **Please note** that settings for this option are disabled (grayed out) if you are using the free version.

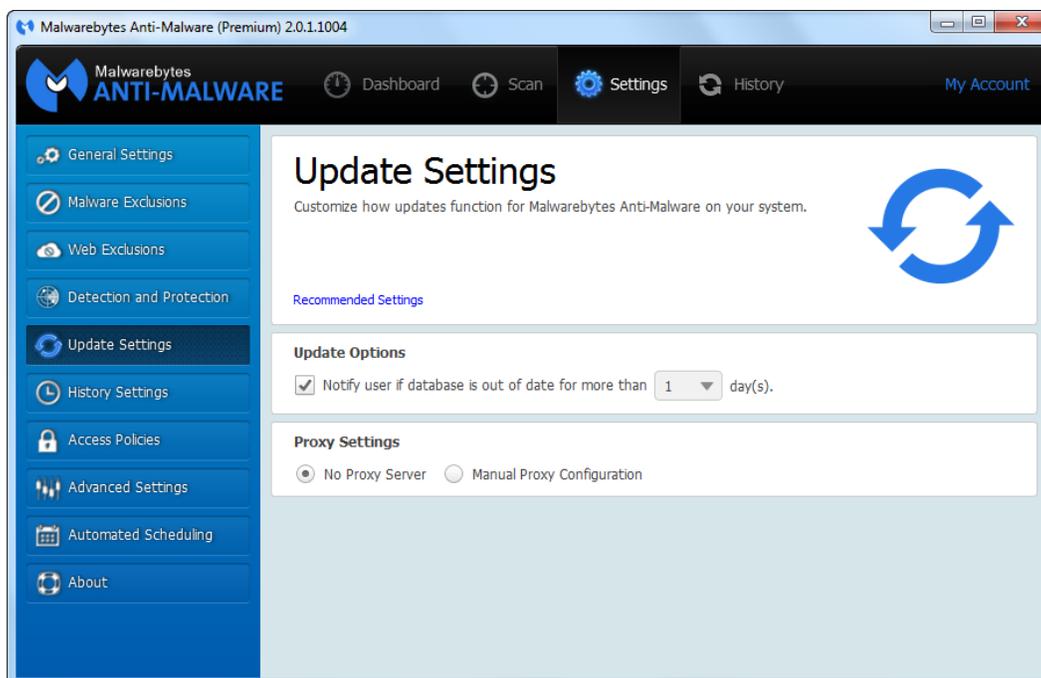
### **6.4.4 Malicious Website Protection (Premium/Trial versions only)**

This option allows you to enable or disable protection revolving around websites as a whole. This option does not treat different protocols differently. It does not distinguish between your favorite game being served on one port and a potential malware source being served on another. Should you choose to disable this feature, you could inadvertently compromise your computer's safety. **Please note** that settings for this option are disabled (grayed out) if you are using the free version.

## **6.5 Update Settings**

---

This screen allows configuration of update settings for your Malwarebytes installation. A screenshot of this module is shown here, with recommended (default) settings displayed.



### 6.5.1 Update Options

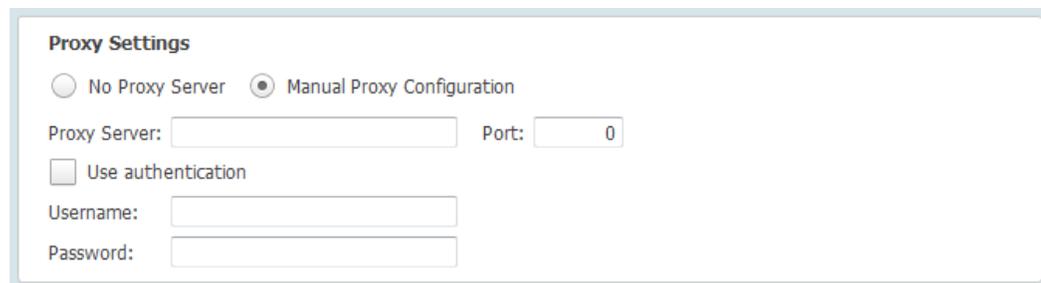
You may specify if you will be notified if your rules database is out of date, and if so, how many days in arrears it may be before you are notified. The date range is adjustable between one (1) and twenty-eight (28) days. We recommend that you do not allow the rules database to become dated, as much damage is caused by zero-day infections – those threats that are too new to be adequately protected against by anti-virus software.

**Please note** that users of Malwarebytes Anti-Malware free version must manually initiate a database update, using the *Dashboard*. Automatic updates are available only to users of the Premium or Trial versions.

### 6.5.2 Proxy Settings

This setting determines whether connections to the public internet (for database and program updates) will use a proxy server in conjunction with that access. In a home environment, only advanced users utilize proxy servers, and then on a limited basis. They are more often used on a corporate network. They have two primary purposes. The first is to funnel all communications to and from the outside world through a single connection point, thus assuring anonymity of all computers on the corporate network. The second purpose is to utilize *content caching*. This means that any external content which had recently been requested by any user could be saved locally for some period of time, then subsequent requests by that user (or others) could use the recently-saved data. This method often conserves significant bandwidth, resulting in lower operating costs for companies that use this strategy.

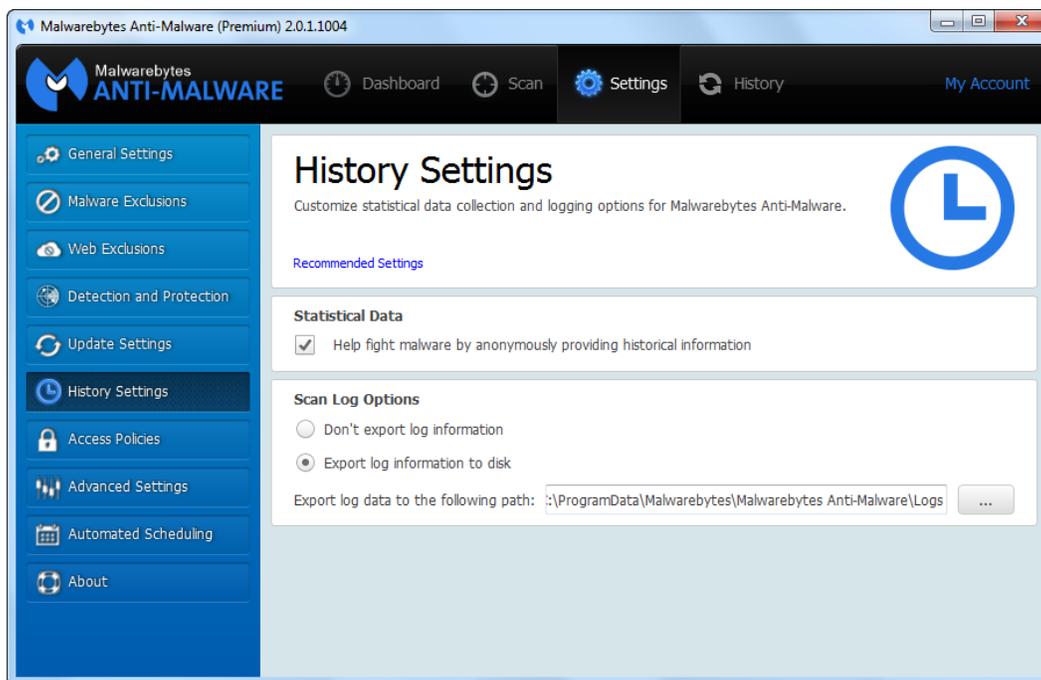
By default, Malwarebytes Anti-Malware does not use a proxy. If configured to do so, the bottom panel will change to provide configuration options as shown below.



You can now specify the IP address or name of a proxy server, as well as the appropriate port number. If a proxy is in use, the name and port number must be specified by the person who controls access to the proxy server. He will also be able to tell you whether authentication is required to use the server, and if so, provide a username and password which have been assigned to you.

## 6.6 History Settings

This screen controls logging options for Malwarebytes Anti-Malware. A screenshot of this module is shown below, with recommended (default) settings displayed.



### 6.6.1 Statistical Data

If you check this box, you will be sending us information that helps us do our jobs. Our Marketing organization likes to know what countries Malwarebytes Anti-Malware is being used in, and the breakdown of subscriptions, trials, and free versions. Our Research organization likes to keep track of what malware we are detecting and how often. We can learn that from what you send us, and that allows us to serve you more effectively. That's all the information we collect, and that's fine with us. We hope that's fine with you as well.

### 6.6.2 Scan Log Options

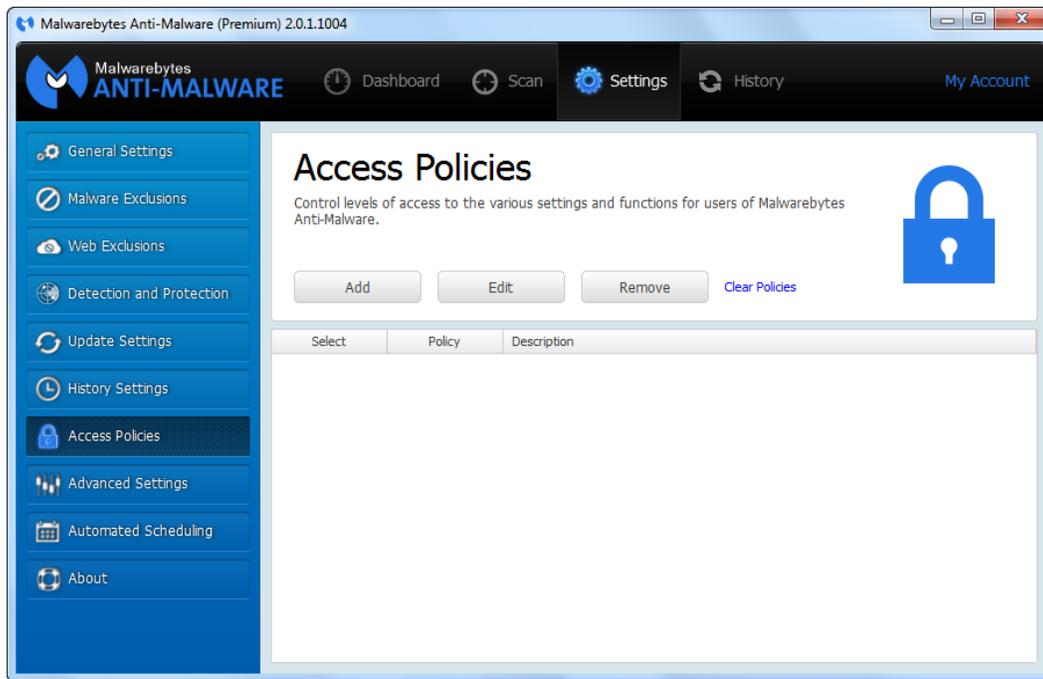
You can choose to **Export log information to disk**. This option and the **Don't export log information** option work together. If one radio button is selected, the other is deselected. If you choose to export log information to disk, it is stored in Extensible Markup Language (XML) format. When exporting logs, you may accept the default path as shown, or specify a new path. Scan logs are stored in:

- **Windows XP:** `C:\Documents and Settings\All Users\Application Data\Malwarebytes\Malwarebytes Anti-Malware\Logs`
- **Other OS versions:** `C:\ProgramData\Malwarebytes\Malwarebytes Anti-Malware\Logs`

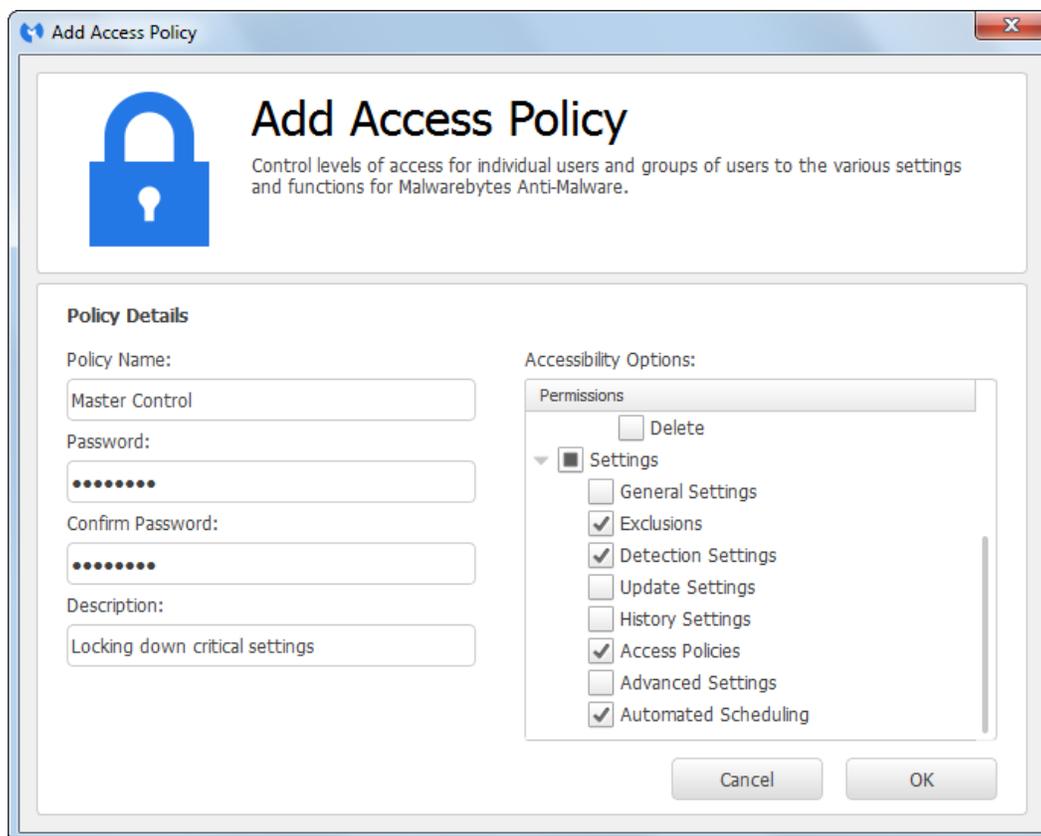
When specifying a new path, clicking the button to the right of the default path brings up a window similar to that used in Windows Explorer. There, you may specify the new path.

## 6.7 Access Policies

This screen allows users of Malwarebytes Anti-Malware Premium and Trial versions to restrict access to various features and functions in Malwarebytes Anti-Malware by protecting them with a password. This feature is not available to users of the free version. Currently, only one policy may be in effect at any given time. A screenshot of this module is shown below.

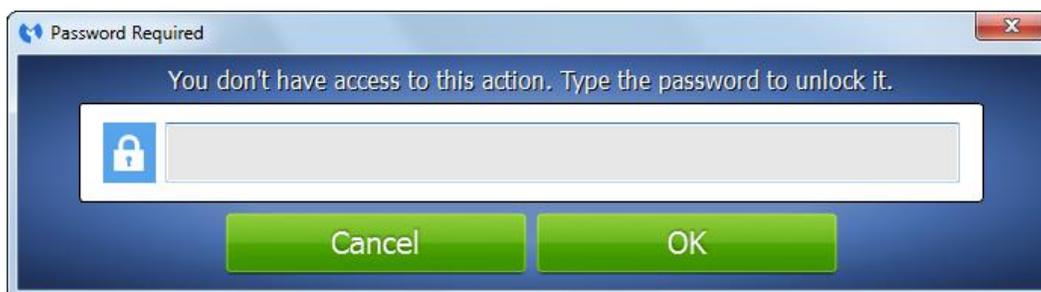


The top portion of the screen provides buttons to allow you to **Add** a new policy, **Edit** or **Remove** an existing policy, or **Clear Policies** as a whole. Let's add a new access policy now by clicking the **Add** button.



The screenshot above shows a newly-created Access Policy. The left half of the screen shows that information to identify the policy has been provided, along with a password. The right side shows the specific functions of Malwarebytes Anti-Malware that are to be controlled by the new Access Policy. Every program function is listed here, but this screenshot shows only those that are to be controlled. The black square in front of *Settings* means that some – but not all – of this group are affected. The checkmarks specify which are affected.

When attempting to gain access to any of the checked areas, you will be required to enter a password (as shown below).

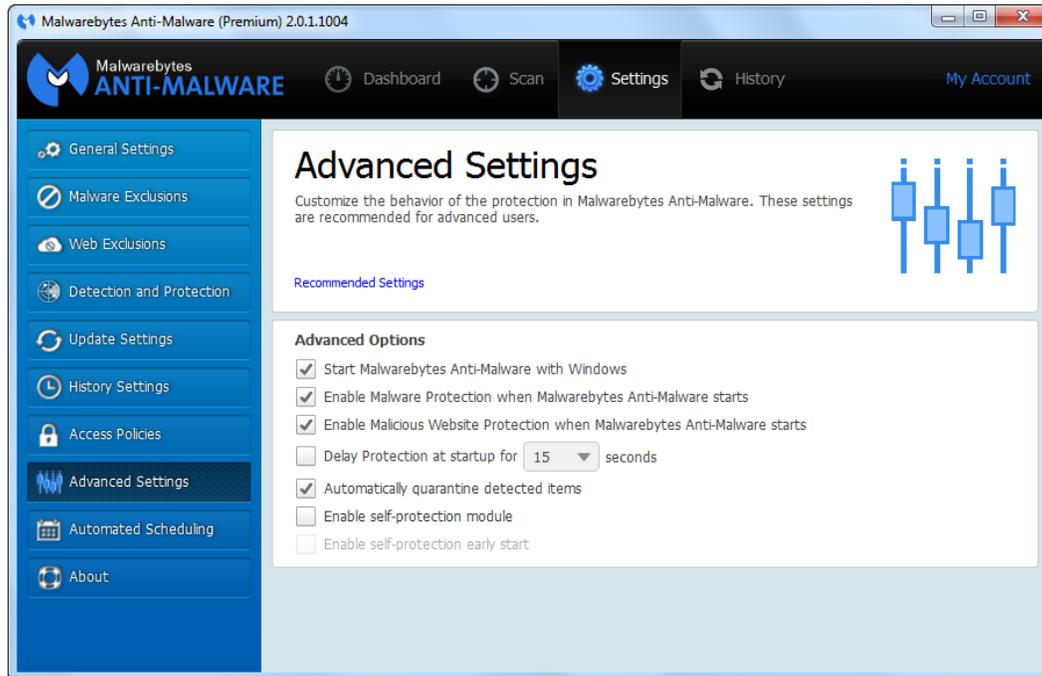


Because Access Policies have been placed under control of the new policy, the password is also required to add, edit, remove or clear policies.

**WARNING:** Please don't forget your password. If you do lose your password, the only way to regain control of password-affected areas is to uninstall and reinstall Malwarebytes Anti-Malware.

## 6.8 Advanced Settings

This screen allows users of Malwarebytes Anti-Malware Premium and Trial versions to control certain protection settings for Malwarebytes Anti-Malware. This feature is not available to users of the free version. Settings which may be changed here are based upon two reasons – compatibility issues with other installed software, or specialized use of Malwarebytes Anti-Malware on your computer. These settings should only be modified by advanced users, or as directed by Malwarebytes Technical Support. A screenshot of this module is shown below, using recommended (default) settings.



Let's look at each of these settings in detail, but with a focus on what's not recommended. Sometimes it's good to know why things are the way they are!

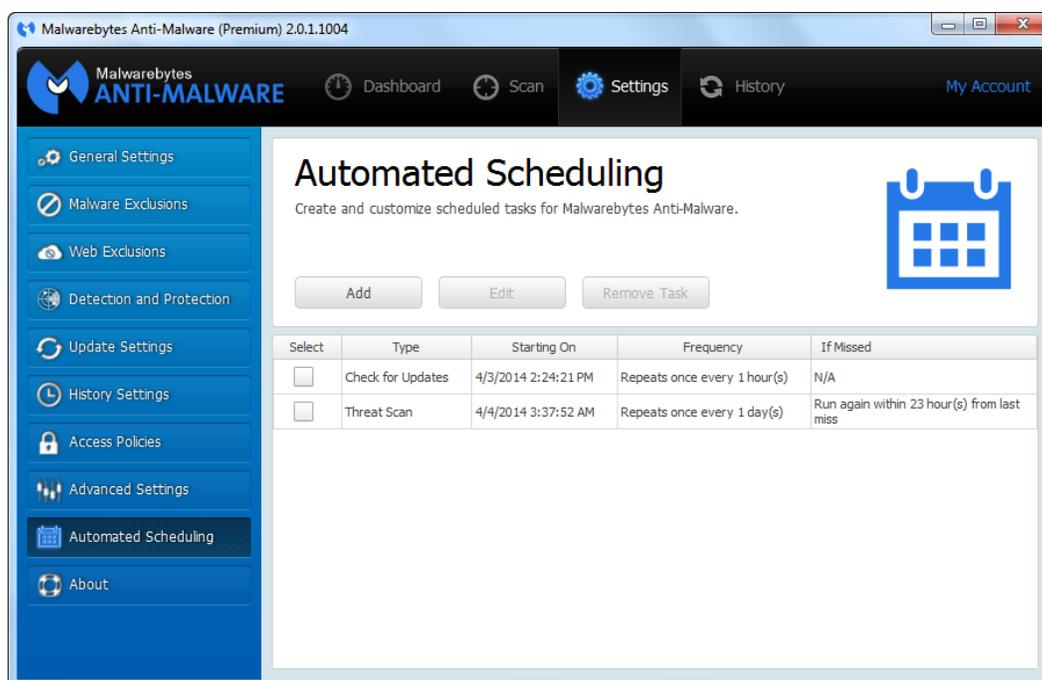
- **Start Malwarebytes Anti-Malware with Windows:** If this setting is unchecked, Malwarebytes Anti-Malware will not start with Windows. You would not have real-time protection available to you, and Malwarebytes Anti-Malware could only provide *after the fact* protection via on-demand scanning. When unchecked, this setting will disable the following two options.
- **Enable Malware Protection when Malwarebytes Anti-Malware starts:** If left unchecked, real-time Malware Protection will not start automatically when Malwarebytes Anti-Malware is launched. This setting does not affect the setting for Malicious Website Protection at program startup. It will override the Malware Protection setting in Detection Settings.
- **Enable Malicious Website Protection when Malwarebytes Anti-Malware starts:** If left unchecked, real-time Malicious Website Protection will not start automatically when Malwarebytes Anti-Malware is launched. This setting does not affect the setting for Malware Protection at program startup. It will override the Malicious Website Protection setting in Detection Settings.
- **Delay Protection at startup for <x> seconds:** There may be times when the startup of system services used by Malwarebytes Anti-Malware conflicts with services required by other applications at boot time. When this is the case, check this box. You will need to experiment with the specific delay setting necessary to compensate for the conflict. When required, this must be done on a case-by-case basis. The delay setting is adjustable from 15-180 seconds, in increments of 15 seconds.
- **Automatically quarantine detected items:** When unchecked, any threats detected will not be quarantined immediately. A notification will instead be presented, and you must choose how to respond. If you do not

respond within forty (40) seconds, the threat will still be quarantined, but the possibility (however small) exists that the threat could have become active within that timeframe.

- **Enable self-protection module:** This setting controls whether Malwarebytes Anti-Malware creates a *safe zone* to prevent malicious manipulation of the program and its components. Checking this box introduces a delay as the self-protection module is enabled. While not a negative, the delay may be considered undesirable by some users. When unchecked, the "early start" option which follows is disabled.
- **Enable self-protection early start:** When the self-protection module is enabled, you may choose to enable or disable this option. When enabled, the self-protection module will become enabled earlier in the computer's boot process – essentially changing the order of services and drivers associated with your computer's startup.

## 6.9 Automated Scheduling

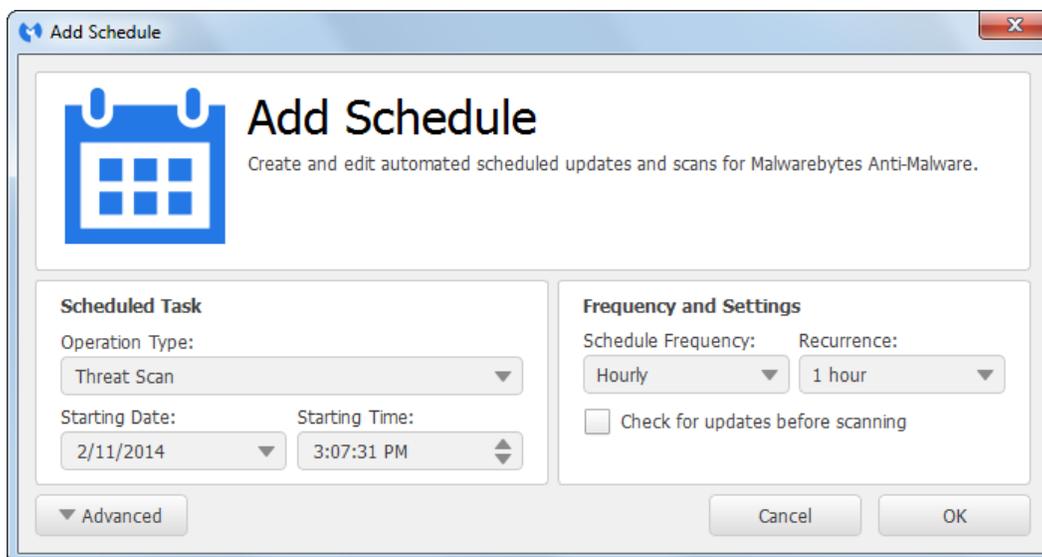
This screen allows users of Malwarebytes Anti-Malware Premium and Trial versions to add, edit and remove scheduled tasks to be executed by Malwarebytes Anti-Malware. This feature is not available to users of the free version. Two types of tasks can be executed by Malwarebytes – scans and updates. A screenshot of this module is shown below.



One scan and one update are defined when Malwarebytes Anti-Malware is installed. You are free to modify or delete them at will. **Please note** that if either task is deleted without a replacement task being defined, your Malwarebytes Anti-Malware program will not deliver the positive results that you expect. The same methods are used here to add a new task as well as to edit an existing task, so let's **Add** a new task in Basic mode.

### 6.9.1 Basic Mode

A screenshot of the basic [Add Schedule](#) screen is shown here.



You can choose the specific task to be added on the left side of the screen, in the Scheduled Task area. You may choose from the following tasks:

- Threat Scan
- Custom Scan
- Hyper Scan
- Check for Updates

Scan types have been previously discussed in the Scan section of this guide (Section 5). Please refer to that section for further information if desired.

The Frequency and Settings section allows you to define the timeframe (Schedule Frequency) that a task will be executed, and how often (Recurrence). For scans, this translates to:

- Frequency = Hourly, recurrence in range of 1-48 hours
- Frequency = Daily, recurrence in range of 1-60 days
- Frequency = Weekly, recurrence in range of 1-8 weeks
- Frequency = Monthly, fixed setting
- Frequency = Once, fixed
- Frequency = On Reboot, fixed

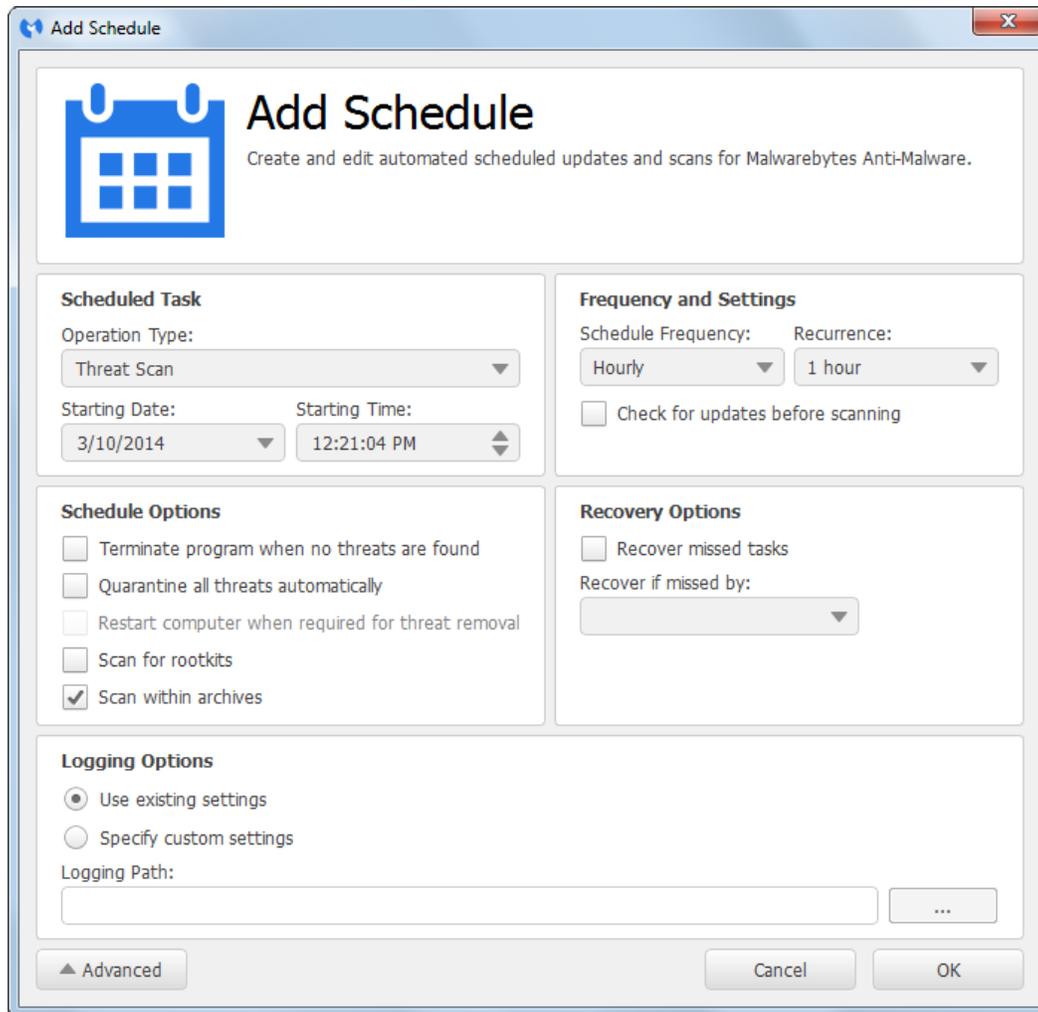
You also have the opportunity to check for updates prior to execution of the scan. We strongly recommend that you always run a scan with the most current database. If you have chosen to define a Check for Updates, the Frequency and Settings variables are:

- Frequency = Realtime, recurrence in range of 1-59 minutes
- Frequency = Hourly, recurrence in range of 1-48 hours
- Frequency = Daily, recurrence in range of 1-60 days
- Frequency = Weekly, recurrence in range of 1-8 weeks
- Frequency = Monthly, fixed setting
- Frequency = Once, fixed
- Frequency = On Reboot, fixed

Our Research group updates the Rules database anywhere from 8-15 times daily (unless there is a specific reason to update more often). Based on this, there is really no reason to check for updates more often than once per hour.

## 6.9.2 Advanced Mode

At the bottom left corner of the Add Schedule window is the **Advanced** button. Click that to expand the Add Schedule window to expose several more options. A screenshot is shown below.



In Advanced Mode, we add options which allow you to tailor the task more to your liking. Let's look a little deeper, beginning with the advanced options for scans.

## 6.9.3 Advanced Scan Options

Schedule Options provides several added capabilities to the basic settings which have already been described. Here's a rundown on the advanced options.

- **Terminate program when no threats are found:** We do not recommend selection of this option if you are using the Premium or Trial version of Malwarebytes Anti-Malware. Doing so would leave you without real-time protection.
- **Quarantine all threats automatically:** This option determines if a newly-detected threat would be automatically quarantined, or if you would be notified so that you could choose a course of action. While automatic quarantine may seem to be the best course of action, it could have negative implications if a false positive was encountered. A *false positive* is the categorization of a legitimate file as a malicious file. It does rarely occur, and when it does, Malwarebytes Technical Support will assist you in having the offending file evaluated more fully by our Research group.

- **Restart computer when required for threat removal:** This is available only if threats are automatically quarantined, and is not selected by default. Some threats may require a computer restart to completely eliminate the threat, but we feel it's best to notify you at the time, so you may save your work before restarting your computer. If this were checked, you could lose work unless you were monitoring the scan in progress.
- **Scan for rootkits:** This option allows specialized testing for the presence of rootkits. Due to its nature, it increases the required time for a scan to execute.
- **Scan within archives:** This is selected by default. It allows scanning to go three levels deep within archive files.

Recovery Options allow you to recover from a missed task (e.g. your computer was off at the time a scan was to take place).

Selecting the **Recover missed tasks** checkbox activates a selector so that you can specify how long you are overdue before you initiate a scan using this option.

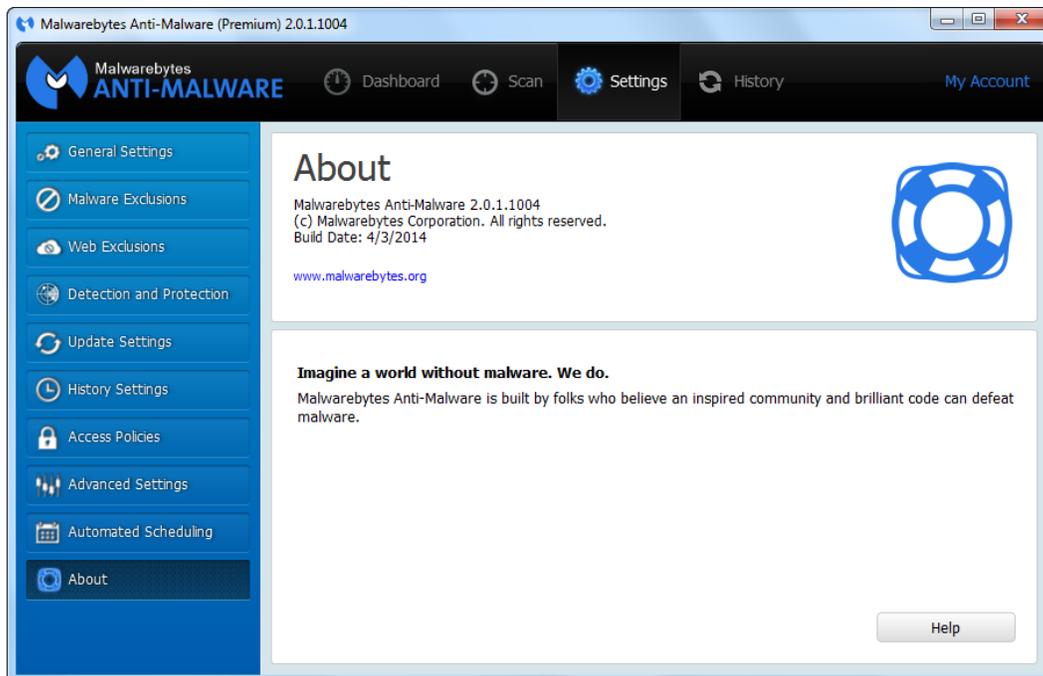
Logging options allows you to use existing settings (as specified in *History Settings*, Section 6.6) or to choose an alternate path.

### 6.9.4 Advanced Update Check Options

Advanced options are limited when checking for updates. Under Schedule Options, you may choose whether a notification appears after a successful rules database update. Recovery Options allows you to perform a database update if you missed your scheduled one, and define what constitutes *overdue*. **Please note** that this option is non-functional if Frequency Settings is set to check for updates on a real-time basis. As with advanced scan options, you may specify an alternate log path and format.

## 6.10 About

The *About* page is simple and straight-forward, and is shown below.



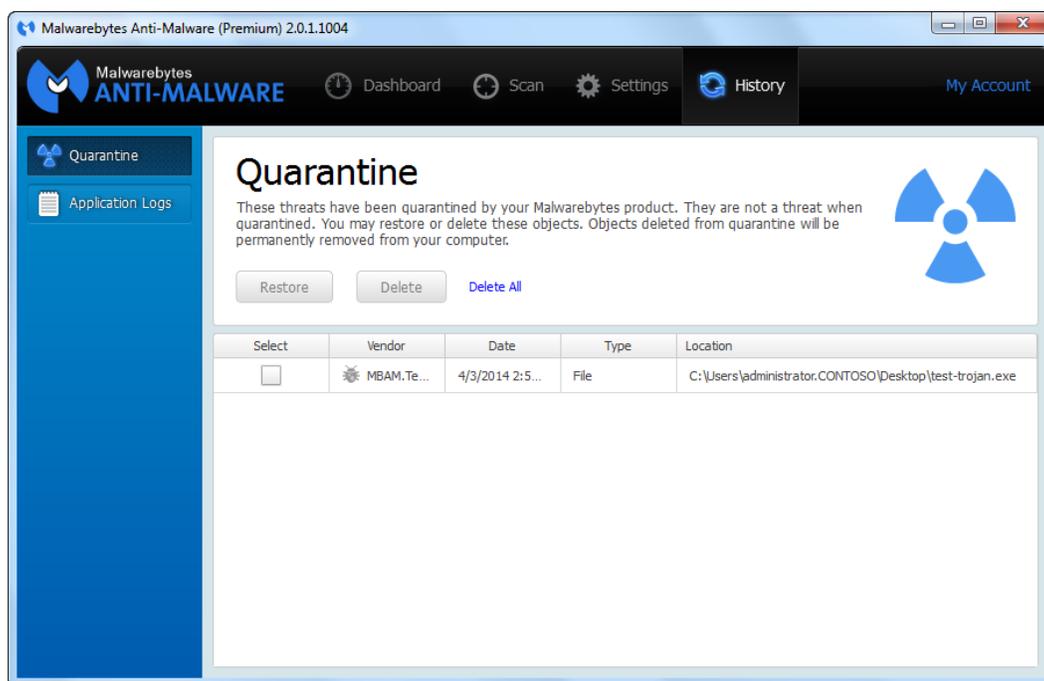
The upper panel contains version information, which is important information when you request Technical Support or are in need of a program update. The lower panel contains a simple statement of our purpose as a company, an abbreviated End User Licensing Agreement (EULA), and finally a **Help** button which, when clicked, brings you to a web-based version of this guide.

## 7.0 History

Malwarebytes Anti-Malware History is divided into two categories which are presented to the user – quarantine and program logs. While a lot of activity happens behind the scenes, the user is primarily interested in whether they are being protected or if problems are preventing the protection they expect. History information presented here provides the desired information.

### 7.1 Quarantine

When executing scans (on-demand or as part of real-time protection), some programs or files may have been categorized as threats. At that time, they were removed from the disk location where they were stored, placed in quarantine, and modified so that they could not pose a threat to your computer. There may be files which fall into this category, but are not malicious. It is up to individual users to research and make this determination. Upon entry to the *History* module of Malwarebytes Anti-Malware, you are presented with the *Quarantine* page, as shown below.

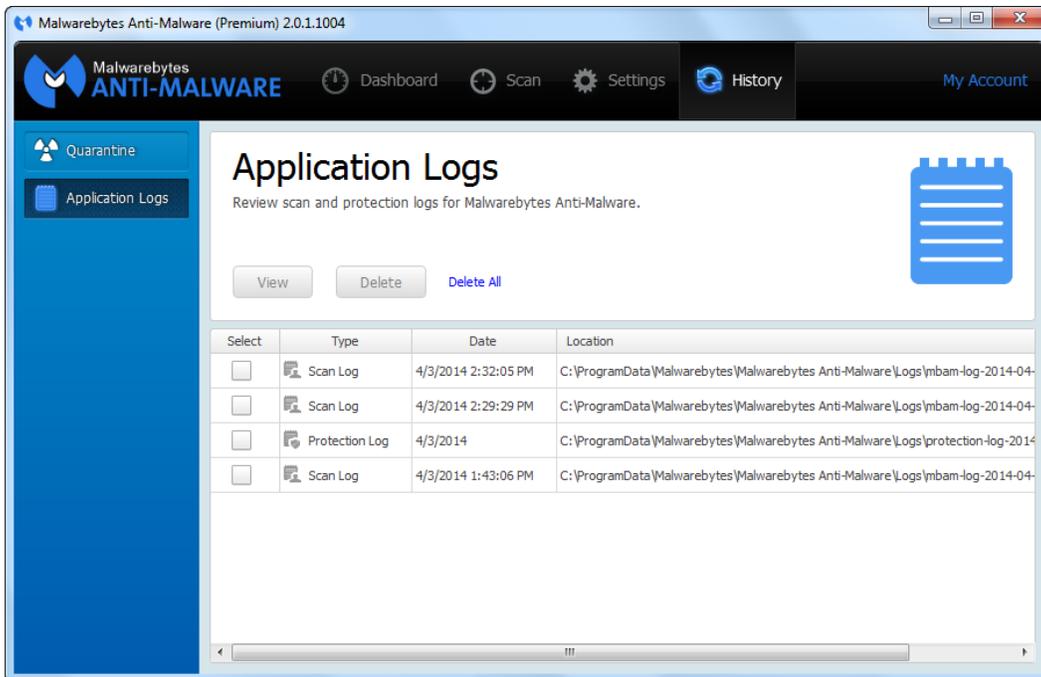


This page allows the user to view the contents of quarantine, and to restore or delete files if desired. Quarantined files are shown in a table format, with pertinent information presented to help you determine what action needs to be taken. Each file listed has a select checkbox in the leftmost column. Checking the checkbox allows you to restore or delete the selected file. Please note that the **Restore** and **Delete** buttons are greyed out until files are selected.

You can choose to **Delete All** quarantined files in a single action. Should there be more than one file in quarantine, you may not restore all files in a single action. Because these files may be malicious, it is intended that you review each file which may be restored before actually doing so. The restored file will continue to be quarantined on future scans unless you add it to the list of files to be excluded from scans in *Malware Exclusions* (Section 6.2).

### 7.2 Application Logs

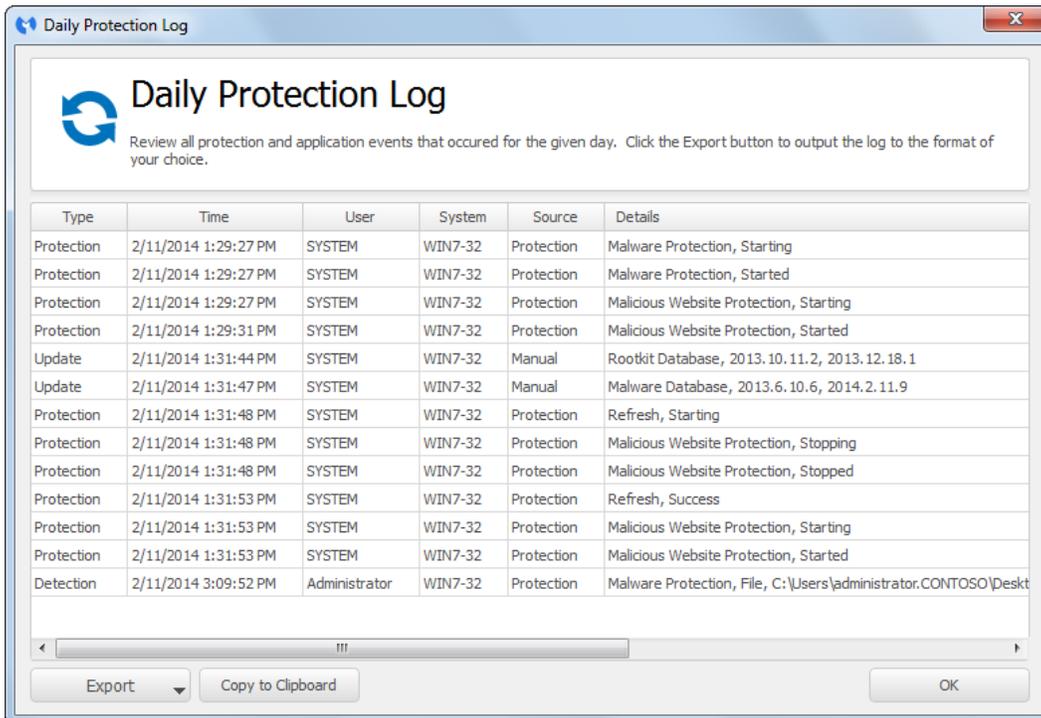
As part of normal program operation, Malwarebytes Anti-Malware produces two different logs. The **Protection Log** is a daily log which itemizes critical events of real-time protection, as well as updates to the Malwarebytes rules database. The **Scan Log** is an event log which shows program configuration and results of each scan that has been executed on the computer which Malwarebytes is installed on. The *Application Logs* program screen is shown here.



This page allows the user to view, export and/or delete these logs. Let's look at these more in depth...

### 7.2.1 Protection Log

The Daily Protection Log shows information in two main categories – update and protection. *Update* entries are typically limited to updates to our rules databases (malware, rootkit), the intelligence behind all Malwarebytes protection. *Protection* entries are related to status changes of real-time protection, as well as integration of updates into real-time protection. A single Protection Log is produced daily, beginning with the first activity which fits log criteria, and updated throughout the day with subsequent activity. The Protection Log is shown below.



By clicking on the headers in the table, you will be able to sort information according to your needs. At the bottom of the Daily Protection Logs, you will also note output options. You may **Copy to Clipboard**, which allows log data to be imported directly into another document. You may also **Export** log data into a number of formats, as listed here:

- **Text file (.txt)** – A generic text file (in comma-delimited format) which may be used directly or input into a program of your choice.
- **Extensible Markup Language (XML) file (.xml)** – A file utilized by XML parsers (or other intermediate processing) to categorize and present data based on requirements of other applications.

### 7.2.2 Scan Log

A Scan Log is created each time that a scan is executed. Scan logs are stored in:

- **Windows XP:** `C:\Documents and Settings\All Users\Application Data\Malwarebytes\Malwarebytes Anti-Malware\Logs`
- **Other OS versions:** `C:\ProgramData\Malwarebytes\Malwarebytes Anti-Malware\Logs`

If you have installed Malwarebytes in a non-standard installation path, these locations will be different. Also, you may have elected to store logs in another location separate from the program installation path. You may confirm that by checking *History Settings* (Section 6.6). Scan logs are (by default) stored in a simple text format. You may modify the log format in *History Settings* (Section 6.6) as well.

### 7.2.3 Viewing or Deleting Logs

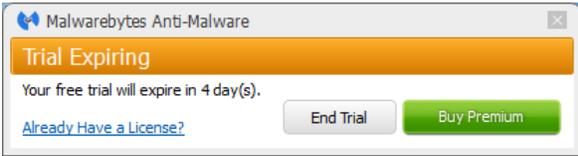
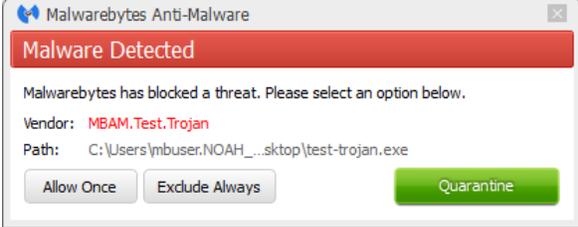
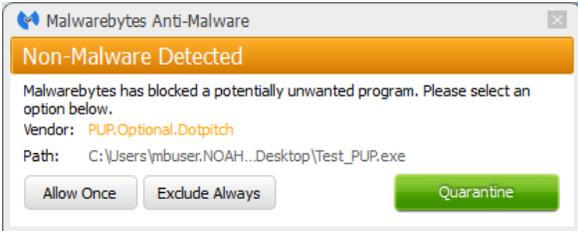
You may view any log file by clicking the log to select it, then clicking the **View** button. As mentioned previously, there are several output options for Protection Logs. A single format is available for Scan Logs, as chosen in *History Settings* (Section 6.6). To delete logs, click the checkbox corresponding to those logs you wish to delete, then click the **Delete** button. To delete all logs at once, click the **Delete All** button. When deleting all logs, you do not need to select any specific logs to enable this action.

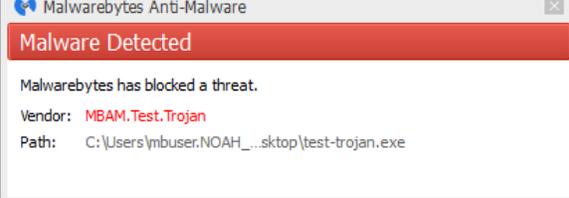
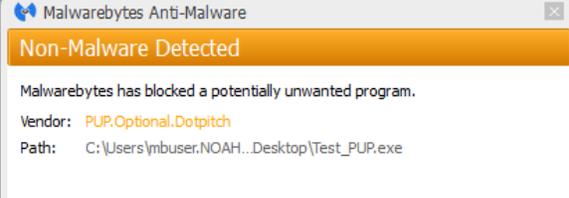
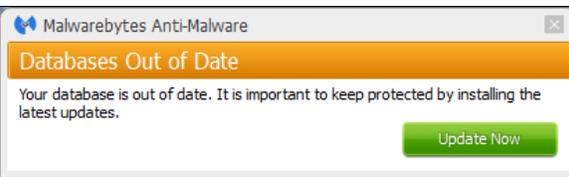
Please bear in mind that computers which have significant threat activity will also have logs of significantly larger size. You should periodically check how much disk space is being used for logs, so that logs do not impact normal operation of your computer.

This page left intentionally blank

## Appendix A: Notification Window Examples

Malwarebytes Anti-Malware provides a number of user notifications during operation. These notifications are always positioned in the lower right corner of your screen. The length of time that they will remain on your screen is configurable in *General Settings* (Section 6.1).

	<p>The free trial period for the product is expiring within days. You may choose to end the free trial period, purchase the annual subscription (which provides full access to all product features), or wait until the product expires to make your choice. If you already have purchased a license but have not yet activated the product, you may click the link at the lower left to do so now.</p>
	<p>The Malwarebytes free trial is in danger of expiring. This will terminate real-time protection, the ability to schedule scans, and automatic updates of the rules database. You may still execute scans on demand. You may also update your Malwarebytes rules database on demand. You may choose to end the free trial period, purchase the annual subscription (which provides full access to all product features), or wait until the product expires to make your choice. If you already have purchased a license but have not yet activated the product, you may click the link at the lower left to do so now.</p>
	<p>Malware has been detected as a function of real-time protection. You have not chosen to exercise the auto-quarantine capability when malware has been detected, so no specific action has been taken. The program now being detected as malware may be acceptable to you, so you may choose to allow its operation once, always, or elect to quarantine it at this time.</p>
	<p>Software classified as <i>Non-Malware</i> has been detected as a function of real-time protection. This software is typically referred to as a Potentially Unwanted Program (PUP) or Potentially Unwanted Modification (PUM). You have not chosen to ignore this class of software, or to exercise the auto-quarantine capability when it has been detected, so no specific action has been taken. The non-malware detection may be acceptable to you, so you may choose to allow its operation once, always, or elect to quarantine it at this time.</p>

	<p>An attempt has been made by software present on your computer to contact a website which is suspected to be malicious in nature. The attempt has been blocked. This detection occurred as a function of real-time protection. This notification provides information which may help you to determine whether the connection should or should not be allowed. You may choose to exclude the website, which will allow future connections without this notification being displayed.</p>
	<p>Malware has been detected as a function of real-time protection. You have chosen to exercise the auto-quarantine capability when malware has been detected, so the offending software has been moved to quarantine and modified so that it may not cause any damage to your computer.</p>
	<p>A Potentially Unwanted Program (PUP) has been detected as a function of real-time protection. You have chosen to exercise the auto-quarantine capability when a PUP has been detected, so the offending software has been moved to quarantine and modified so that it may not cause any damage to your computer.</p>
	<p>A scan (scheduled or on-demand) has been completed. Malware was detected during execution of the scan. Clicking the notification will allow you to review the scan log to determine the exact nature of the threat(s).</p>
	<p>A scan (scheduled or on-demand) has been completed. Non-Malware was detected during execution of the scan. This is typically a Potentially Unwanted Program (PUP) or Potentially Unwanted Modification (PUM), which may be acceptable to you. Clicking the notification will allow you to review the scan log to determine the exact nature of the threat(s).</p>
	<p>One or both aspects of real-time protection are disabled. You may re-enable protection by clicking the <b>Fix Now</b> button, or within <i>Detection and Protection</i> settings in the user interface. Please note that this notification and remedial actions apply only to users of Malwarebytes Anti-Malware Premium and Trial versions.</p>
	<p>The Malwarebytes rules database is out of date. You may click the <b>Update Now</b> button to cause an immediate update. Failure to update the database will cause subsequent scans to use outdated protection rules, which could jeopardize the safety of your computer.</p>