Malwarebytes 3

Malwarebytes User Guide

Version 3.1

10 May 2017

Malwarebytes

Notices

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

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. Information about each third party/open source project used in Malwarebytes software – as well as licenses for each – are available on the following page.

https://www.malwarebytes.com/support/thirdpartynotices/

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.

CWC04-3010a

Table of Contents

Introduction

Malwarebytes 3 is an "AV replacement." It is not an AV. It does not incorporate the same old engine for file-infectors and other malware that you find in a typical AV or Internet security suite, the large and inefficient library of signatures, or the bloatware features which are becoming more prevalent.

You don't need to pay for a traditional AV anymore! At Malwarebytes, we have always approached things differently and, as many people know based on their own positive experience with Malwarebytes finding and remediating malware that gets past AVs, we know a thing or two about zero-day malware and their infection tactics. We have always believed that no one product can do it all, and the free AV that comes with modern operating systems, in conjunction with Malwarebytes is all you will ever need.

In today's modern threat world, bad guys have learned how to evade AV protection, making it more important than ever before to be able to disrupt attacks in as many different stages of the attack chain as possible. *Malwarebytes 3*, layered with the AV (which is the default mode) or as your stand-alone defense, is the most effective approach against modern threats. And if all else fails, you need the best remediation technology available.

Malwarebytes 3 has been engineered to provide the most effective layered approach of prevention, detection and remediation technologies:

1. Application hardening, to make them more resilient against attacks.
2. Anti-exploit technology, to shield applications from vulnerability exploits (currently one of the top infection vectors).
3. Application Behavior Enforcement, an advanced and signature-less technology which prevents common infection vectors (e.g. web & email based social engineering).
4. Anti-ransomware, a signature-less technology designed for frictionless mass market adoption after a huge beta process.
5. Revamped Anti-Malware and Web Blocking engines, offering more aggressive detection techniques with tighter False Positive controls to allow us.
6. Hardened and modular architecture design, allowing seamless integration of new detection and protection technologies in the future.
7. Highly effective as always in malware remediation, an often overlooked part of the protection stack.
8. Ability to run as primary protection (no AV) or secondary protection (alongside existing AV).
9. Engineered to be our next corporate endpoint client, providing major improvements to our endpoint management capabilities and new enterprise-focused offerings
10. Last but not least, our Research Team has been growing and adapting lately, with notable additions to the lineup from *JRT* and *AdwCleaner*, our new aggressive stance against PUPs, as well as new R&D technologies which we will be unveiling shortly.

Welcome to the *Malwarebytes 3* User Guide!

What's New in Malwarebytes 3.1

This version of *Malwarebytes* contains many improvements and bug fixes. Following is a list of changes.

Performance/protective capability

- Multiple enhancements result in reduction of memory usage
- Faster load time and responsiveness of third-party applications
- Improved performance of Web Protection
- Faster Malwarebytes 3 program startup time and responsiveness of user interface
- New detection and protection layer with machine learning based anomaly detection (to be deployed gradually even if it shows "enabled" under Settings)
- Improved Self-Protection by requiring escalated privileges to disable protections or deactivate a license
- Enhanced malware protection techniques and remediation capabilities
- Added an automatic monthly scheduled scan in Free mode

Usability

- Added ability to control the priority of manual scans on the system
- Added setting to turn off 'Real-Time Protection turned off' notifications when protection was specifically disabled by the user
- Added ability to exclude the last website blocked by Web Protection via the tray menu
- Fixed several defects related to configuring Custom Scans, including selecting child folders and fixing issues with touch screens
- Fixed problem where a right-click context scan appeared broken after scheduled scan due to misleading "Cannot start a scan while another one is in progress" message
- Fixed issue where you could not add or edit a scheduled scan in Spanish and some other languages
- Fixed issue where scan could appear stuck on Heuristics Analysis when it had actually completed successfully
- Fixed issue where Self-Protection setting would fail to toggle correctly after an upgrade

Stability/issues fixed

- Fixed several crashes in the Web Protection module
- Fixed issue where Ransomware Protection would be stuck in 'Starting' state after a reboot
- Fixed a conflict with Norton that caused web pages not to load and plug-ins to crash in Chrome
- Fixed issue with WMI protection technique in Exploit Protection that could cause Office applications to crash
- Fixed several crashes related to the service and tray
- Fixed security vulnerabilities that could be chained together to perform local privilege escalation
- Fixed many other miscellaneous defects and user interface improvements

System Requirements

Following are minimum requirements for a computer system on which *Malwarebytes 3* 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 (Service Pack 1 or later, 32/64-bit), Windows XP (Service Pack 3 or later, 32-bit only)
- **CPU:** 800 MHz or faster, with SSE2 technology. This includes most modern Intel x86 processors as well as AMD's Athlon 64, Sempron 64, Turion 64 and Phenom CPU families. Please refer to the following page for further information:

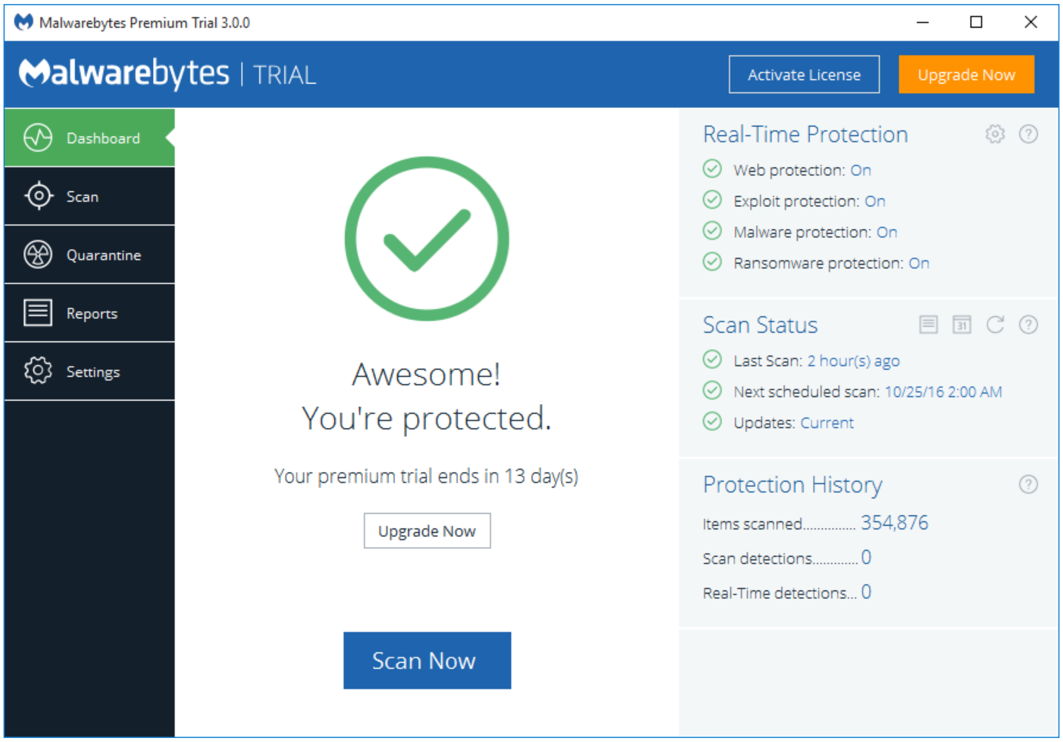
  https://en.wikipedia.org/wiki/SSE2
- **RAM:** 2048 MB (64-bit OS), 1024 MB (32-bit OS, except 256 MB for Windows XP)
- **Free Disk Space:** 250 MB
- **Recommended Screen Resolution:** 1024x768 or higher
- **Active Internet Connection**

Installation

To begin the installation, double-click on the *Malwarebytes 3* installation file which you downloaded. If you are installing *Malwarebytes 3* 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 3* 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 3* at this time in Free Trial mode.

At this point, program installation is complete. You will see the user interface as shown below. If you have already purchased a license, you may wish to activate your copy of *Malwarebytes 3* at this time. You can do that now (or at any time) by clicking the **Activate License** button at the top right portion of the *Malwarebytes* 3 user interface.



Awesome!
You're protected.

Your premium trial ends in 13 day(s)

Real-Time Protection

Web protection: On
Exploit protection: On
Malware protection: On
Ransomware protection: On

Scan Status

Last Scan: 2 hour(s) ago
Next scheduled scan: 10/25/16 2:00 AM
Updates: Current

Protection History

Items scanned.............. 354,876
Scan detections............ 0
Real-Time detections... 0

Free, Trial or Premium?

Before you begin, we want to let you know that throughout this guide, you will see references to the Free, Trial, and Premium versions of *Malwarebytes 3*. This is likely unfamiliar territory for new *Malwarebytes* users. The following link provides a basic rundown on the differences between the Free and Premium versions of *Malwarebytes 3*.

https://www.malwarebytes.com/trial/#comparison-chart

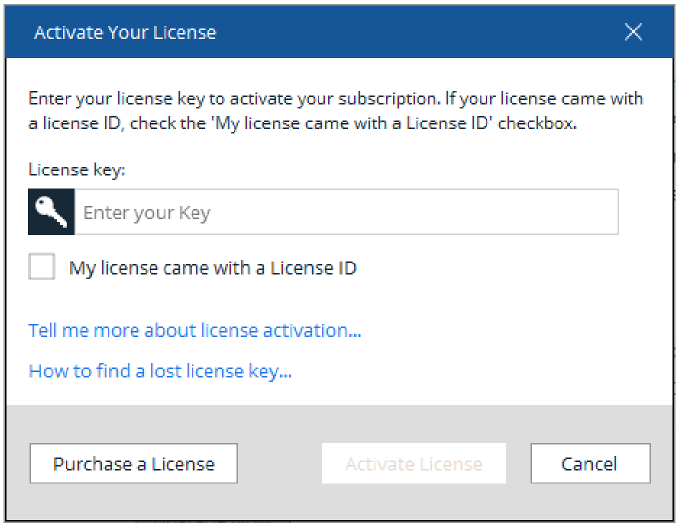
The Trial is a 14-day opportunity to use the Premium version of the program, and to see if it is better suited to your needs. The Trial is available at no cost, but you can only use it one time for each version of *Malwarebytes*. The Free Trial is automatically started during installation. Once installed, the program provides options to convert from Free to Premium, and from Trial to Premium.

If you elect to use the Trial and do not wish to purchase a Premium subscription at the end of the trial, your *Malwarebytes* program will revert to Free mode. The only differences will be that the added features enabled by the trial will cease to function. All other functionality remains unchanged.

Activation

Malwarebytes 3 is available for users of any modern Windows client 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 and access policies. If no license has been installed into the product, the blue title bar at the top of the screen will show two buttons, **Activate License** and **Upgrade Now**. When clicked, **Upgrade Now** 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.

Your license information will be in an email sent to you by Malwarebytes at the time of purchase. Locate your license information and click the **Activate License** button. You will then see the following screen.


Activate Your License

Enter your license key to activate your subscription. If your license came with a license ID, check the 'My license came with a License ID' checkbox.

License key:

Enter your Key

□ My license came with a License ID

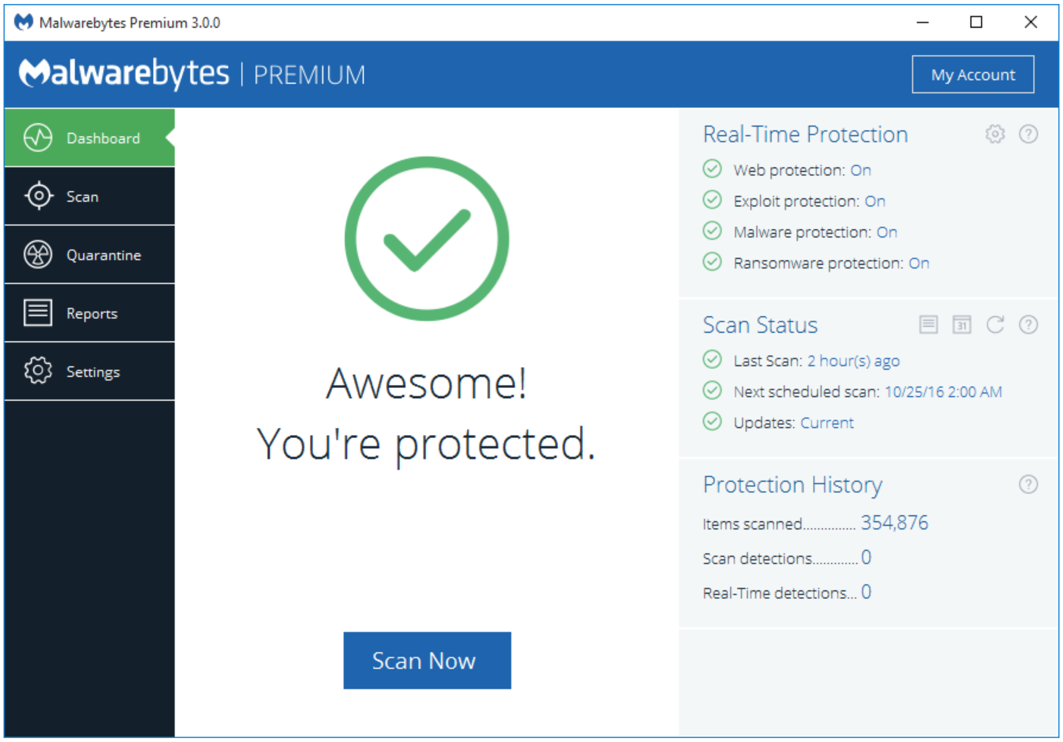
Tell me more about license activation...

How to find a lost license key...

Please note the checkbox and the words "My license came with a License ID." If you are using our "old style" license, you will also need to check that box and enter your **License ID** along with your **Key**.

Please note: You must be online with an active Internet connection in order to successfully activate your Premium license.

The construction of the Key is different, so make sure that you choose the right screen for entering your license information based on whether you have an **ID** and **Key**, or just a **Key**. After entering your license information, click the **Activate License** button. Your *Malwarebytes 3* screen will refresh, as shown below.



Awesome!
You're protected.

Real-Time Protection

- ✓ Web protection: On
- ✓ Exploit protection: On
- ✓ Malware protection: On
- ✓ Ransomware protection: On

Scan Status

- ✓ Last Scan: 2 hour(s) ago
- ✓ Next scheduled scan: 10/25/16 2:00 AM
- ✓ Updates: Current

Protection History

Items scanned..............	354,876
Scan detections............	0
Real-Time detections...	0

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 Premium Trial 3* to *Malwarebytes Premium 3*.

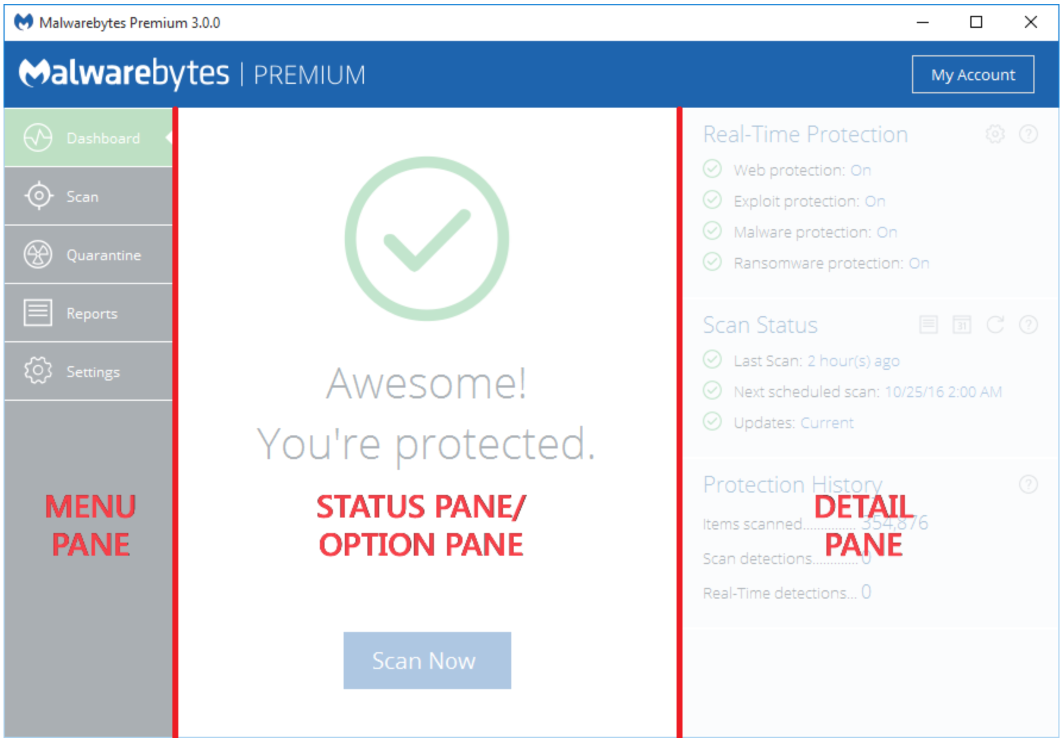
A Final Word about Administrative Rights

If you installed *Malwarebytes* from a downloaded installation file, you automatically started a Premium Trial, and was offered 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.

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

Screen Layout

The *Malwarebytes 3* 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 Dashboard – the screen you see when *Malwarebytes 3* is launched for the first time.



Awesome!

You're protected.

Web protection: On

Exploit protection: On

Malware protection: On

Ransomware protection: On

Last Scan: 2 hour(s) ago

Next scheduled scan: 10/25/16 2:00 AM

Updates: Current

Items scanned............ 354,876

Scan detections............ 0

Real-Time detections... 0

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

Menu Pane

The Menu Pane 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.
- **Quarantine:** Delete or restore threats which have been detected by program scans.
- **Reports:** View reports related to program operation, threats which have been detected, and threats which have been removed.
- **Settings:** Configure every aspect of *Malwarebytes 3*, so that it can protect you efficiently.

In addition, there are settings for Account information. While in Premium Trial mode, options are present to buy a Premium subscription and to **Activate** the program. 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.

Status/Option Pane

When the Dashboard is selected from the Menu Pane, the center of the screen is filled with the Status Pane. It is designed to give you quick information that tells you whether there is anything for you to be concerned about. When the Dashboard is selected, the Detail Pane is also displayed. More on that momentarily.

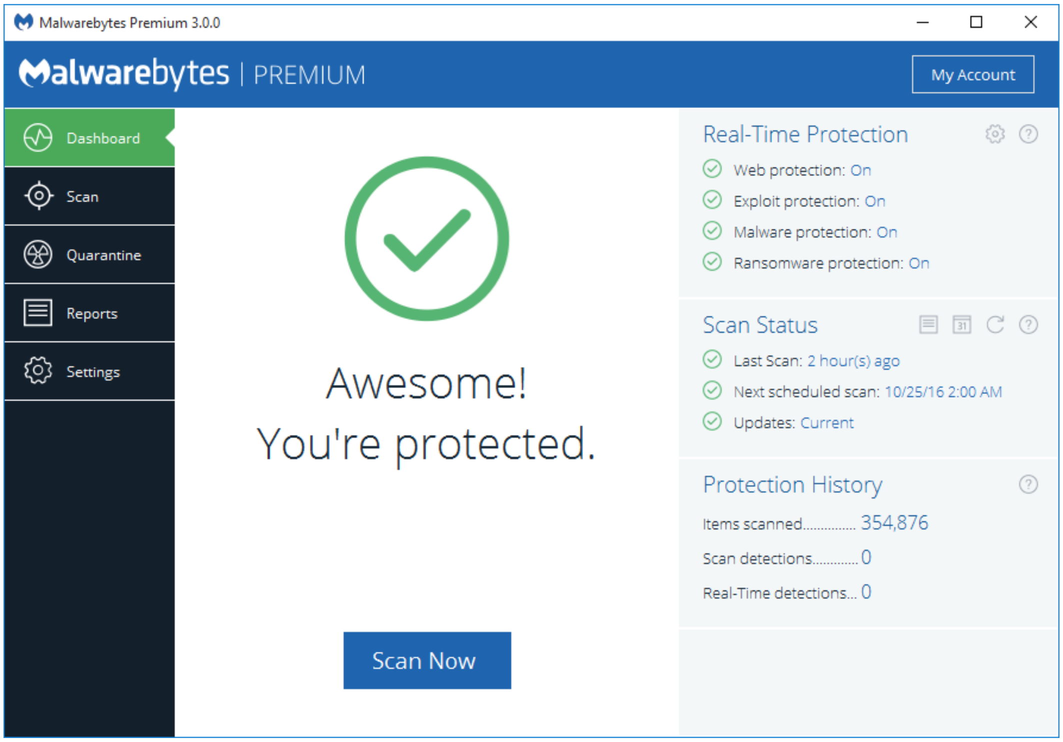
When any menu option other than the Dashboard is selected, all space except the space used by the Menu Pane is allocated to the selected menu option. This provides sufficient room for information pertaining to any menu option to be cleanly displayed.

Detail Pane

The Detail Pane is shown only when the Dashboard is selected. It shows information on protection options, protection updates, and detail pertaining to the most recent scan. This information is shown on other screen displays as part of the menu option selected by the user, but are all displayed here for quick recognition.

Dashboard

Each time *Malwarebytes 3* is launched, the first page visible to the user is the *Dashboard*. It is designed to provide program 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.



Awesome!
You're protected.

Real-Time Protection
- Web protection: On
- Exploit protection: On
- Malware protection: On
- Ransomware protection: On

Scan Status
- Last Scan: 2 hour(s) ago
- Next scheduled scan: 10/25/16 2:00 AM
- Updates: Current

Protection History

Items scanned...............	354,876
Scan detections.............	0
Real-Time detections...	0

Status Pane

The main area of the screen is the Status Pane, providing current system status. Within the Main Window, the first item displayed is the Status Banner. This banner displays a status message along with an icon, whose color is based on program status. The color is meant to alert the user to conditions which may require intervention. Colors used 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)**
  - Awesome! You're protected. (Premium mode and Premium Trial modes which will expire more than 7 days in the future)
  - You're running Malwarebytes Free 3. (free mode only)
- **Color: orange (non-critical problem)**
  - You're not fully protected.
  - Your Protection Updates are not current.
  - Your program version is out of date
  - Your Premium Trial ends in <x> days. (trial expiring in 4-7 days)
  - Your subscription ends in <x> days (subscription ending in 8-30 days)
- **Color: red (critical problem)**
  - Your Premium trial ends in <x> days. (trial expiring in 0-3 days)
  - Your subscription ends in <x> days (subscription ending in 0-7 days)
  - We were unable to renew your subscription (renewal failed, and you are now in 30-day grace period)

Real-Time Protection

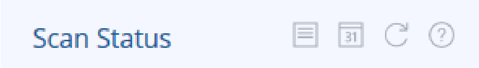
This item shows the status for each of the four Real-Time Protection features. If you are in Premium Trial mode, it is enabled unless you click the **End Free Trial** button. **Please note** that real-time protection is enabled only for *Malwarebytes Premium 3* and *Malwarebytes Premium Trial 3* users. This feature is not available if you are using the Free version.

Settings

Settings are accessed by clicking the small gear at the top right of the Real-Time Protection panel. When clicked, the Settings screen will be displayed, allowing access to all program settings. Please refer to the *Settings* portion of this guide (pages 22-36) for complete information on this topic.

Scan Status

This panel shows your scanning activity at a glance. You can easily see when the last scan was completed, when the next scan is scheduled, and the status of your protection updates. There are four icons on the title bar for this panel, as shown here.



A description for each icon is as follows.

View Scan Reports

This icon takes you to Reports, where you can view detailed reports on scans which *Malwarebytes 3* has performed on your computer. Please note that information shown here is limited to the last scan that was executed. See the Reports Pane (pages 19-21) for information on reports as a whole.

Schedule a Scan

The second icon allows scans to be scheduled for automatic execution. This option is available only for *Malwarebytes Premium 3* and *Malwarebytes Premium Trial 3* users. The icon remains visible in Free mode, but clicking it has no effect. When clicked, the Settings screen will be displayed, allowing access to the Scan Schedule screen. Please refer to the *Scan Schedule* portion of this guide (pages 30-31) for full information on this topic.

Check for Updates

The third icon causes *Malwarebytes 3* to connect with Malwarebytes servers to check for protection updates more current than those in use, and download them if they exist. This option is functional for all program modes.

Help

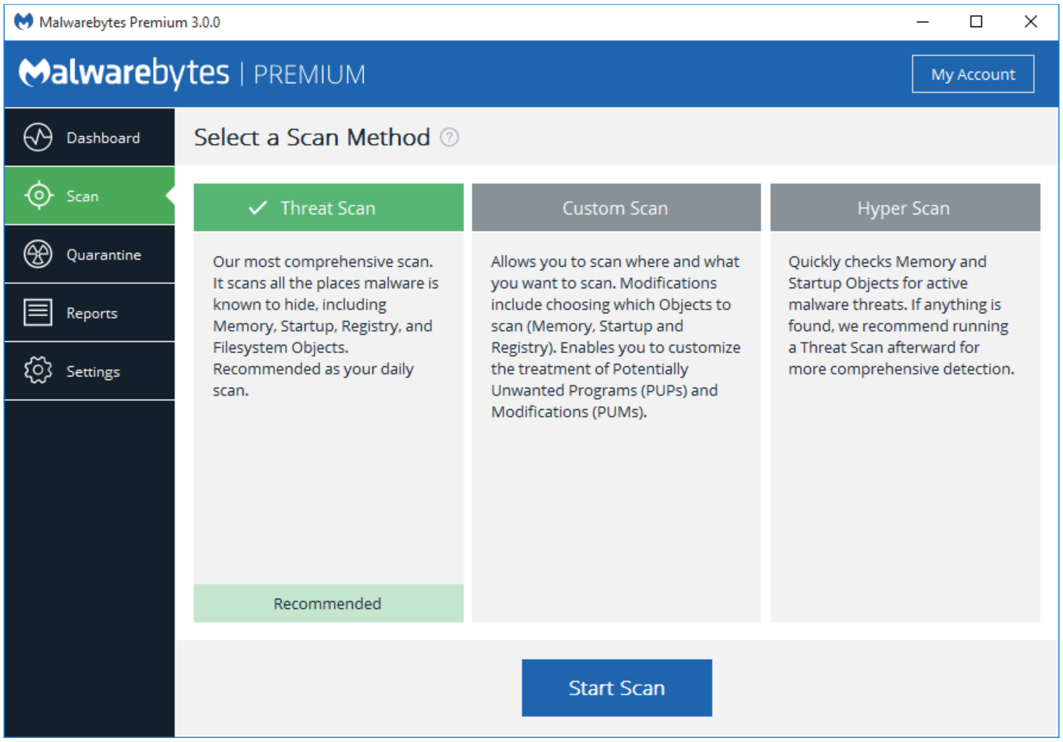
The fourth icon links to the *Malwarebytes 3 User Guide* on the Malwarebytes website. This behavior is consistent throughout the program.

Protection History

This panel shows three key statistics. It shows how many items were scanned, how many threats were detected during scans, and how many threats were detected by real-time protection. Please note that the number of items scanned includes individual files that are part of archive files, as well as components in dynamic link library (DLL) files. Also note that real-time detections can only occur in Premium and Trial modes.

Scan

The Scan Pane is the introduction to scan-related options in the program. When you click **Scan** in the Menu Pane, you will see the screen shown below.



Threat Scan: Our most comprehensive scan. It scans all the places malware is known to hide, including Memory, Startup, Registry, and Filesystem Objects. Recommended as your daily scan.

Custom Scan: Allows you to scan where and what you want to scan. Modifications include choosing which Objects to scan (Memory, Startup and Registry). Enables you to customize the treatment of Potentially Unwanted Programs (PUPs) and Modifications (PUMs).

Hyper Scan: Quickly checks Memory and Startup Objects for active malware threats. If anything is found, we recommend running a Threat Scan afterward for more comprehensive detection.

There are three scan types which can be executed – Threat Scan, Custom Scan, and Hyper Scan. Hyper Scan is only available to users of the Premium or Trial modes. Please note that global scan settings used by Threat Scans and Hyper Scans are selected in Settings (see pages 31-32). Following are more detailed descriptions of each of the scan modes.

Threat Scan

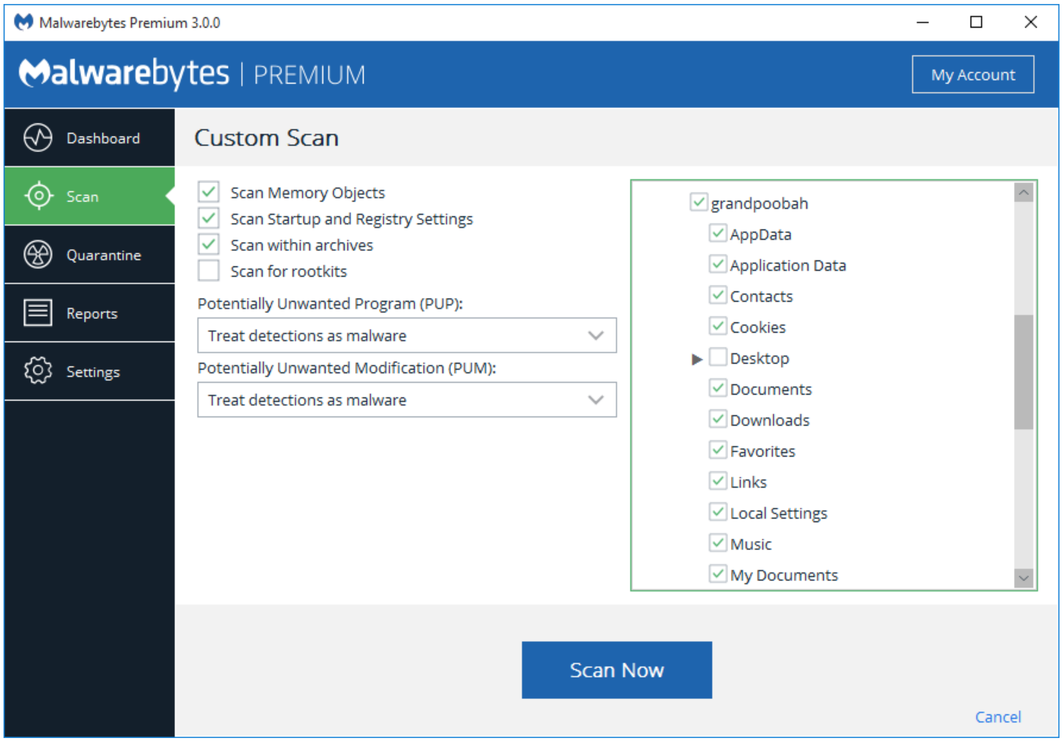
This method of scanning detects a large majority of threats that your computer may be faced with. Areas and methods tested include:

- **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.
- **File System 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.

The *Threat Scan* is the scan method which we recommend for daily scans. While it will not scan every file on your computer, it will scan the locations which most commonly are the launch point for a malware attack.

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. These settings will override scan settings defined elsewhere. A screenshot of the custom scan configuration screen is shown below.



Custom Scan

☑ Scan Memory Objects
☑ Scan Startup and Registry Settings
☑ Scan within archives
☐ Scan for rootkits

Potentially Unwanted Program (PUP): Treat detections as malware

Potentially Unwanted Modification (PUM): Treat detections as malware

- ☑ grandpoobah
  - ☑ AppData
  - ☑ Application Data
  - ☑ Contacts
  - ☑ Cookies
  - ▶ ☐ Desktop
  - ☑ Documents
  - ☑ Downloads
  - ☑ Favorites
  - ☑ Links
  - ☑ Local Settings
  - ☑ Music
  - ☑ My Documents

Custom Scanning Options

These settings provide capability to determine the functional areas that will be scanned. They are as follows:

- **Memory Objects:** Memory which has been allocated by operating system processes, drivers, and other applications. It is important to note that threats detected during scans are still considered threats if they have an active component in memory. As an extra measure of safety, memory objects should be scanned.
- **Startup and Registry Objects:** Executable files and/or modifications which are initiated at computer startup, as well as registry-based configuration changes that can alter startup behavior.
- **Archives:** If this setting is checked, archive files (ZIP, 7Z, RAR, CAB and MSI) will be scanned up to four levels deep. Encrypted (password-protected) archives cannot be tested. If left unchecked, archive files will be ignored.
- **Rootkits:** These are files stored on your computer's local disk drives which are invisible to the operating system. These files may also influence system behavior.

Potentially Unwanted Programs/Modifications

These settings allow the user to choose how Potentially Unwanted Programs (PUPs) and Potentially Unwanted Modifications (PUMs) will be treated if they are detected.

Folders to be Scanned

This setting allows the user to include or exclude directories, subdirectories, and individual files from scans. It utilizes a Windows Explorer-like presentation model. In the screenshot shown above, every directory except Desktop is selected for a custom scan. You may scan parent directories separately from child directories based on individual selections.

Hyper Scan

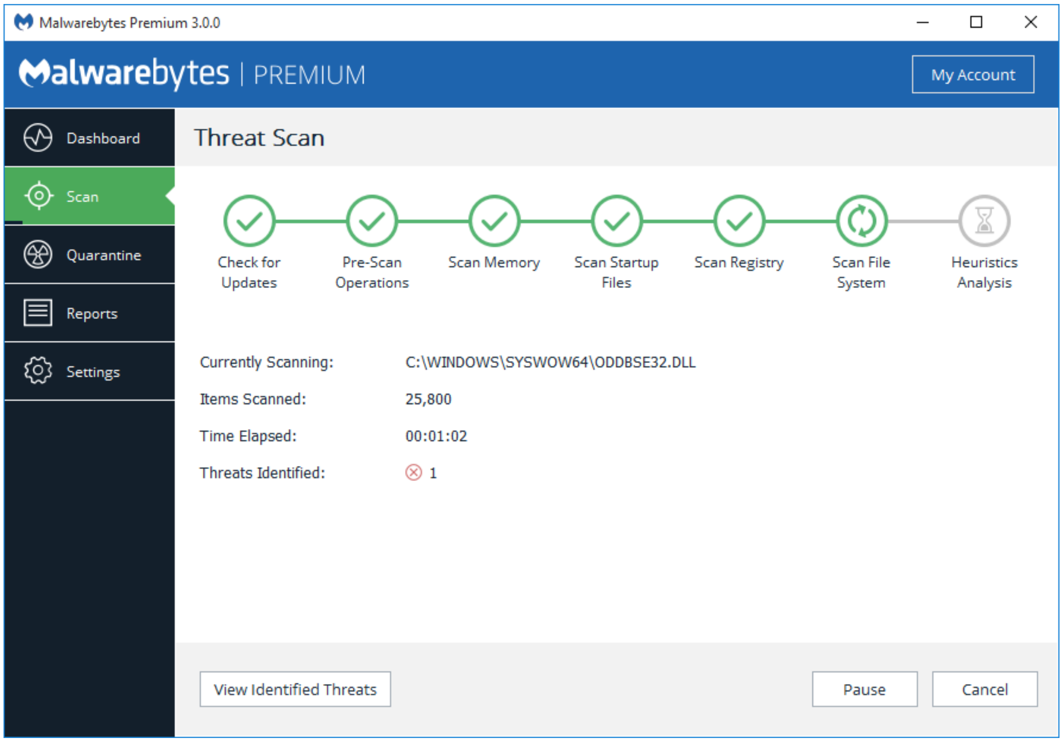
This scanning option is only available to users of *Malwarebytes 3 Premium* and *Malwarebytes 3 Trial* versions. This method of scanning is limited to detection of immediate threats. Areas and methods tested include:

- **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.

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.

Watching Scan Progress

Each scan method requires a different amount of time to complete. Unless significant changes have occurred on your local disk, a Hyper Scan or Threat Scan should each be rather consistent from scan to scan. A custom scan time interval may vary widely each time, based on the areas scanned, the number of files involved, and the size and complexity of the files. The screenshot below is an example of a scan in process.



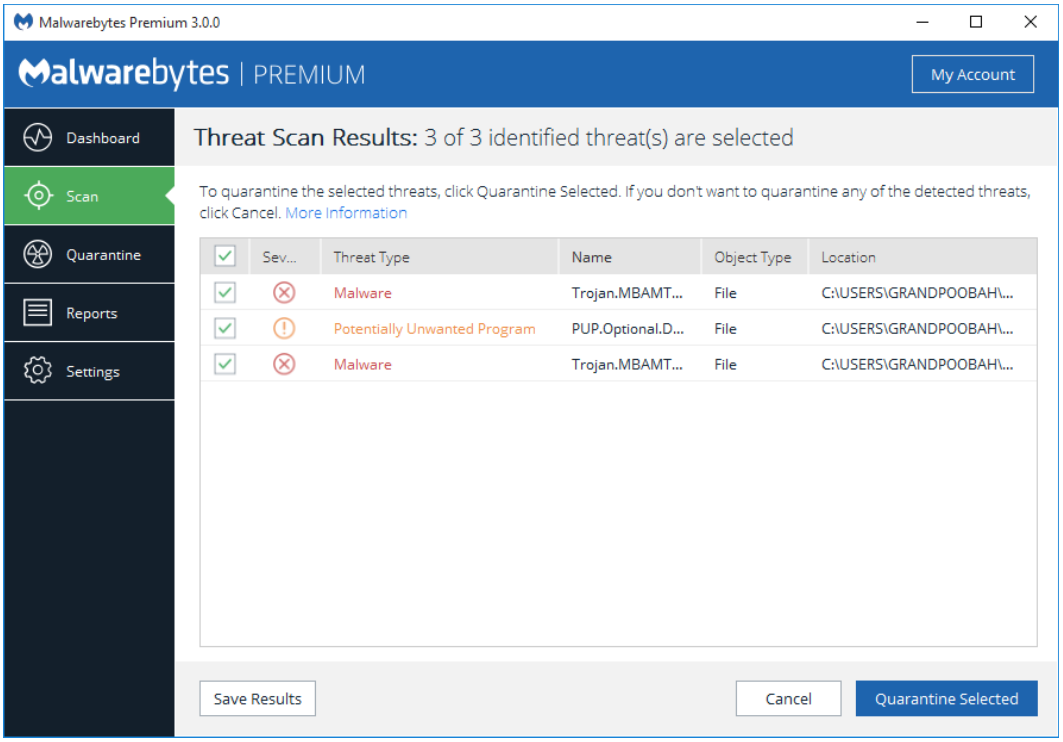
Currently Scanning: C:\WINDOWS\SYSWOW64\ODDBSE32.DLL
Items Scanned: 25,800
Time Elapsed: 00:01:02
Threats Identified: ⊗ 1

The progress bar shows milestones for each phase of the scan, with each milestone represented by a green or gray symbol. In this screenshot, most milestones are shown with green checkmarks, indicating that phase of the scan has been completed. *Scan File System* is represented by an animation which indicates that this phase of the scan is currently being performed. The last milestone – a gray exclamation point – is yet to be completed. All phases which have not been started are initially shown with a grey exclamation point.

You may also pause a scan while it is in process by clicking the Pause button. The scan phase in progress will change to indicate that the scan has been paused. Click Resume to continue the scan where it left off. You may also click Cancel at any time to terminate the scan. Results of the scan will be reported as if the scan ran to completion.

Scan Results

After a scan has been executed, Scan Results are displayed as shown here. In this scan, three threats were detected.



Threat Scan Results: 3 of 3 identified threat(s) are selected

To quarantine the selected threats, click Quarantine Selected. If you don't want to quarantine any of the detected threats, click Cancel. More Information

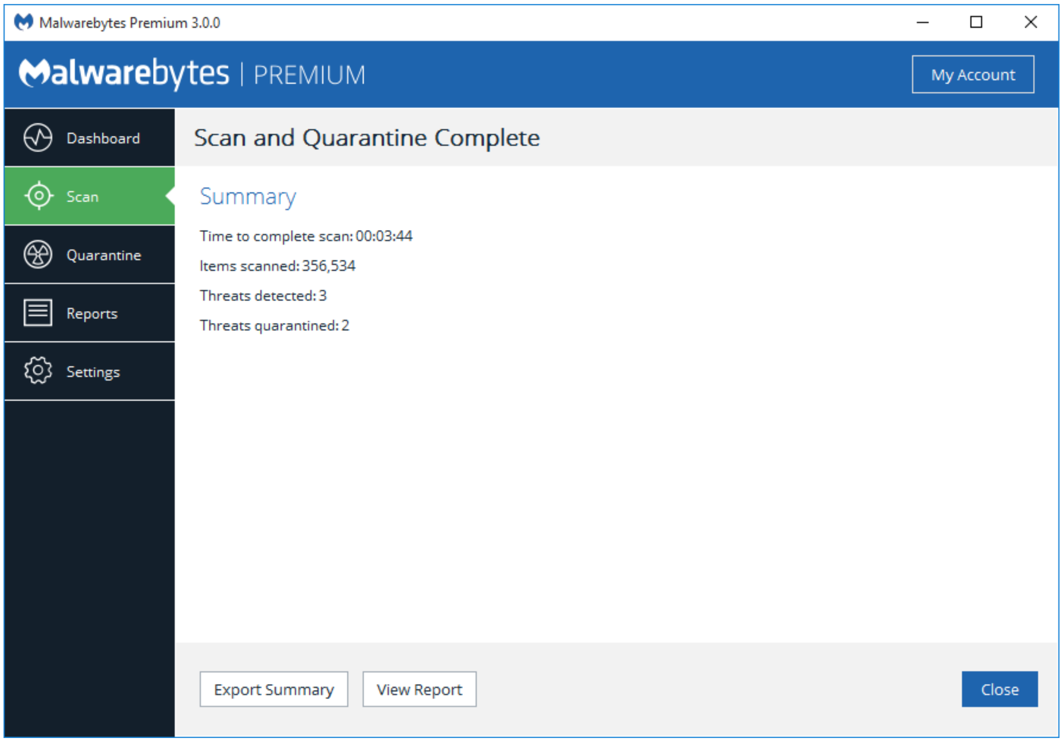
☑	Sev...	Threat Type	Name	Object Type	Location
☑	⊗	Malware	Trojan.MBAMT...	File	C:\USERS\GRANDPOOBAH\...
☑	!	Potentially Unwanted Program	PUP.Optional.D...	File	C:\USERS\GRANDPOOBAH\...
☑	⊗	Malware	Trojan.MBAMT...	File	C:\USERS\GRANDPOOBAH\...

You may move threats to Quarantine by selecting the threat (using checkboxes to the left of the threat's name) and clicking Quarantine Selected. If any threats are not selected to be moved to Quarantine, you will be prompted to Ignore Once, Ignore Always, or Cancel. Ignore Once will result in the threat once again being reported as a threat during the next scan execution. Ignore Always causes the threat to be added to Exclusions. A threat which has been added to Exclusions will no longer be reported as a threat unless there is reason to believe that it has been tampered with. You must provide a disposition for each threat displayed on this screen.

Threats which have been moved into Quarantine cannot harm your computer. They are neutralized as part of the Quarantine process. Please see *Quarantine* (page 18) for further information.

Scan Summary

The final screen to be displayed as part of a scan is the Scan Summary. It provides summary information about the scan, and allows you to view scan detail on screen, or export scan summary or scan detail to a text file. A screenshot of the Scan Summary is shown below.



Scan and Quarantine Complete

Summary

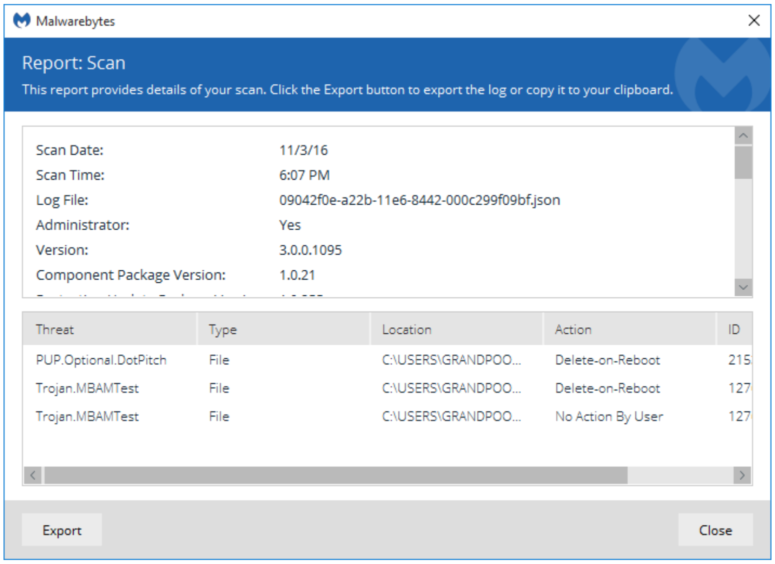
Time to complete scan: 00:03:44

Items scanned: 356,534

Threats detected: 3

Threats quarantined: 2

Clicking the View Report button displays the Scan Report for the scan just completed. It is shown here as well.



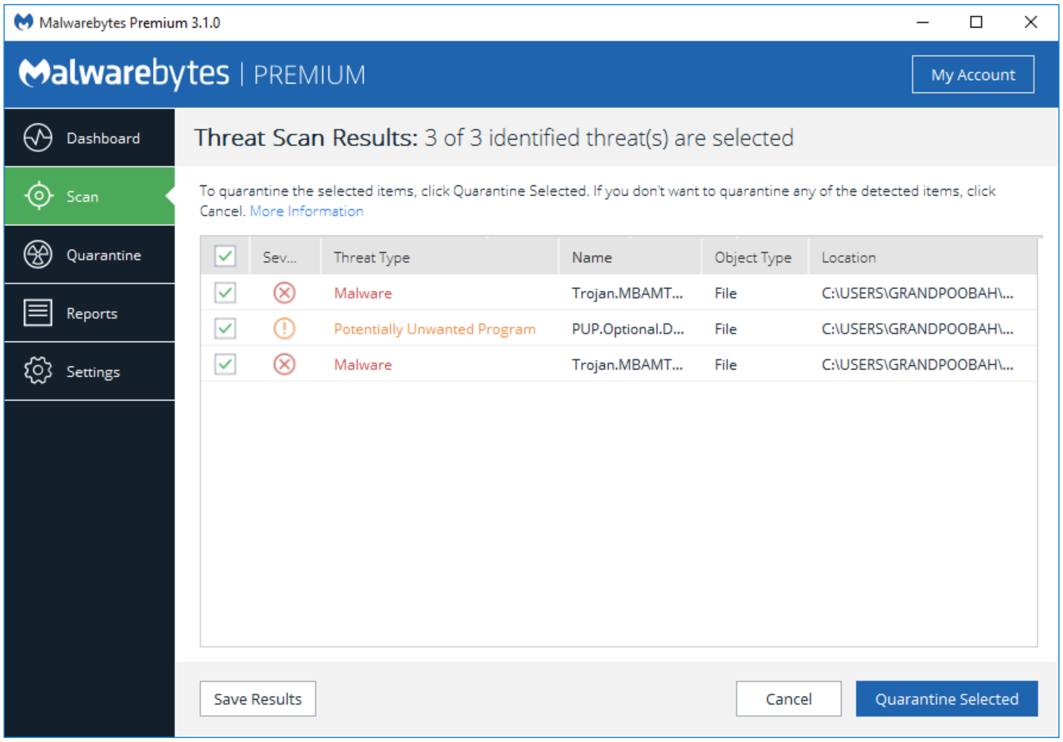
Report: Scan

This report provides details of your scan. Click the Export button to export the log or copy it to your clipboard.

Scan Date:	11/3/16
Scan Time:	6:07 PM
Log File:	09042f0e-a22b-11e6-8442-000c299f09bf.json
Administrator:	Yes
Version:	3.0.0.1095
Component Package Version:	1.0.21

Threat	Type	Location	Action	ID
PUP.Optional.DotPitch	File	C:\USERS\GRANDPOO...	Delete-on-Reboot	215
Trojan.MBAMTest	File	C:\USERS\GRANDPOO...	Delete-on-Reboot	127
Trojan.MBAMTest	File	C:\USERS\GRANDPOO...	No Action By User	127

When threats are detected during a scan, the user must decide how these threats should be handled. The following series of screenshots detail this flow. In the first screenshot, three threats have been detected. By default, all are selected for removal. Please note that the total number of detected threats is shown above the list of threats, and the number of threats that have been selected for removal is shown in red on the same line (near the right edge of the screen).

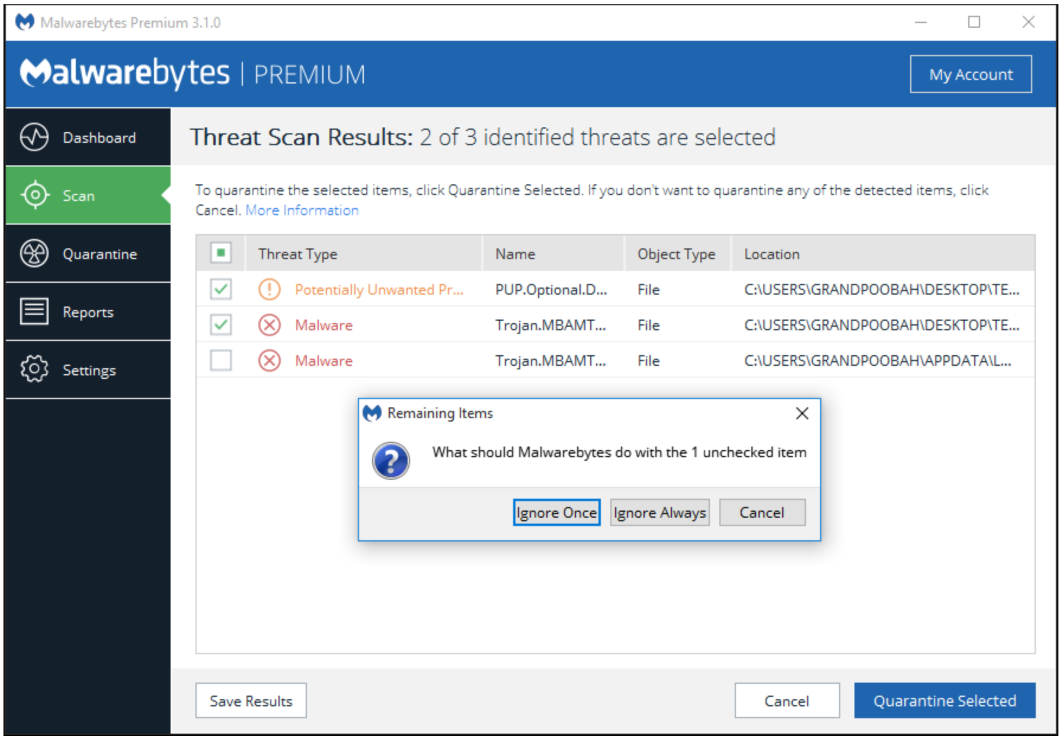


Threat Scan Results: 3 of 3 identified threat(s) are selected

To quarantine the selected items, click Quarantine Selected. If you don't want to quarantine any of the detected items, click Cancel. More Information

☑	Sev...	Threat Type	Name	Object Type	Location
☑	⊗	Malware	Trojan.MBAMT...	File	C:\USERS\GRANDPOOBAH\...
☑	⚠	Potentially Unwanted Program	PUP.Optional.D...	File	C:\USERS\GRANDPOOBAH\...
☑	⊗	Malware	Trojan.MBAMT...	File	C:\USERS\GRANDPOOBAH\...

In order to demonstrate the behavior of this screen, we will uncheck the third threat. This indicates that only the first two threats are to be removed. Clicking the Quarantine Selected button results in the screen shown below.



Threat Scan Results: 2 of 3 identified threats are selected

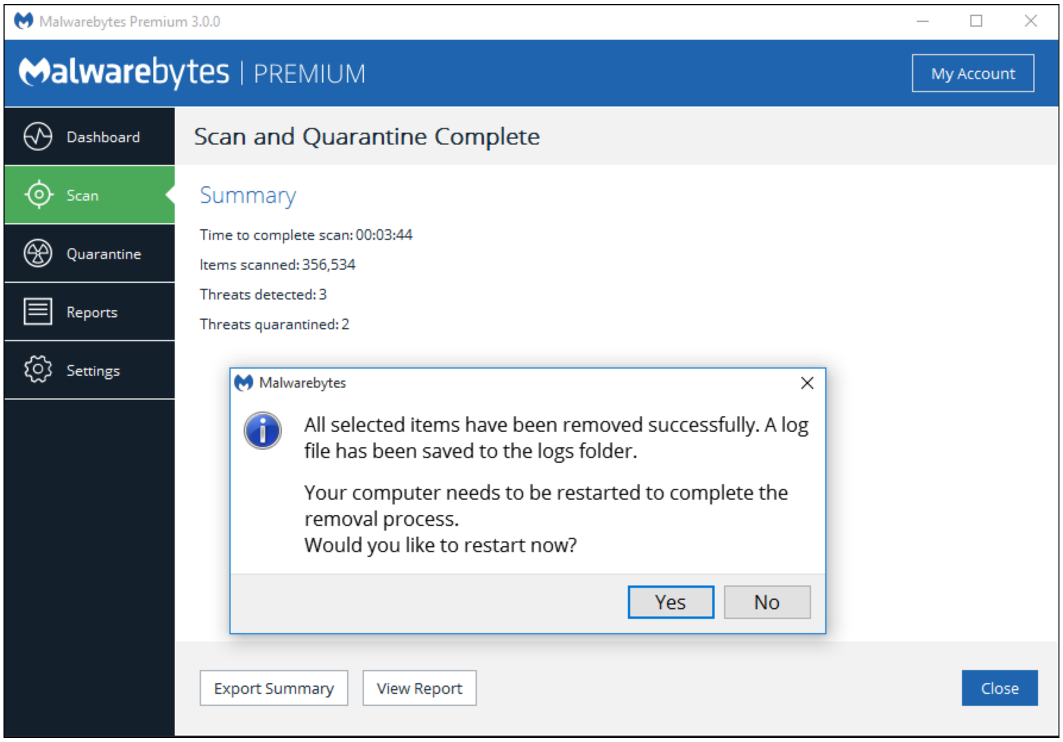
To quarantine the selected items, click Quarantine Selected. If you don't want to quarantine any of the detected items, click Cancel. More Information

■		Threat Type	Name	Object Type	Location
☑	⚠	Potentially Unwanted Pr...	PUP.Optional.D...	File	C:\USERS\GRANDPOOBAH\DESKTOP\TE...
☑	⊗	Malware	Trojan.MBAMT...	File	C:\USERS\GRANDPOOBAH\DESKTOP\TE...
□	⊗	Malware	Trojan.MBAMT...	File	C:\USERS\GRANDPOOBAH\APPDATA\L...

Remaining Items

What should Malwarebytes do with the 1 unchecked item

The threat that was not selected still requires remediation, based on input supplied by the user. In this case, the choices available are Ignore Once, Ignore Always and Cancel. Clicking the Ignore Once button temporarily ignores the threat, although it will be shown as a threat on subsequent scans. Selecting Ignore Always results in the threat being added to the Exclusion List. It would not be scanned in the future. Clicking Cancel keeps you on this screen until you choose how to handle the detected threat. Once a disposition has been selected for all detected threats, the screen below will be displayed.



Scan and Quarantine Complete

Summary

Time to complete scan: 00:03:44
Items scanned: 356,534
Threats detected: 3
Threats quarantined: 2

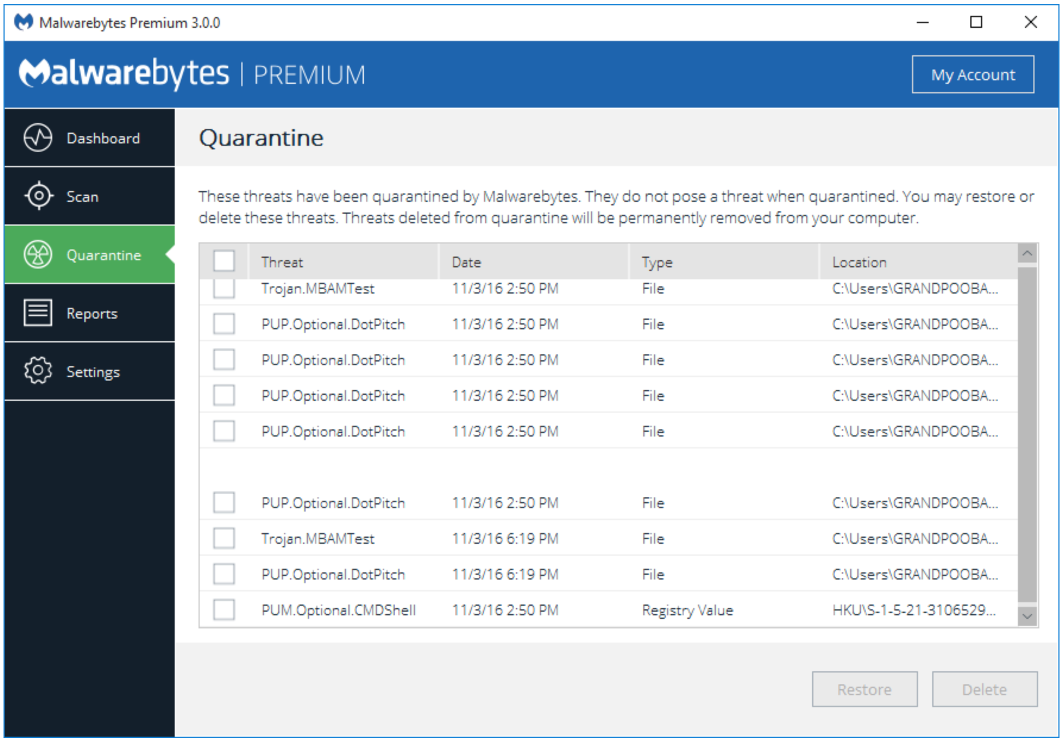
All selected items have been removed successfully. A log file has been saved to the logs folder.

Your computer needs to be restarted to complete the removal process.
Would you like to restart now?

Although a threat has been quarantined, you must restart the computer to assure the threat removal process is complete.

Quarantine

When executing scans (on-demand or as part of real-time protection), some programs, files or registry keys 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 items 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 Quarantine option, you are presented with the screen shown here.



Quarantine

These threats have been quarantined by Malwarebytes. They do not pose a threat when quarantined. You may restore or delete these threats. Threats deleted from quarantine will be permanently removed from your computer.

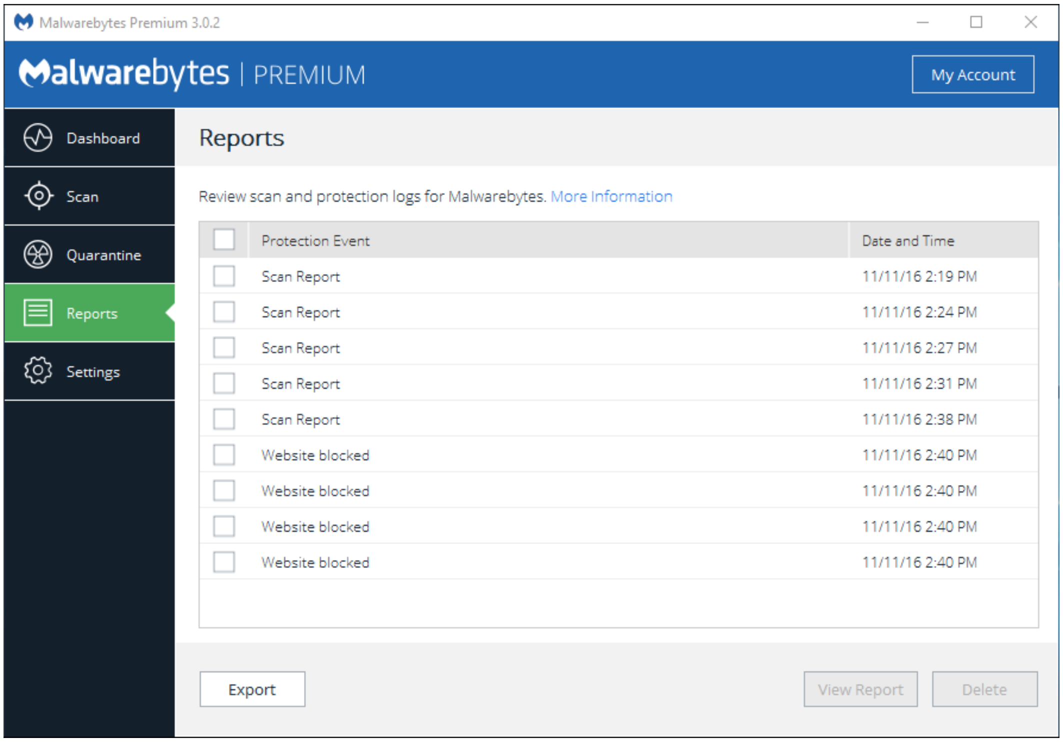
□	Threat	Date	Type	Location
□	Trojan.MBAMTest	11/3/16 2:50 PM	File	C:\Users\GRANDPOOBA...
□	PUP.Optional.DotPitch	11/3/16 2:50 PM	File	C:\Users\GRANDPOOBA...
□	PUP.Optional.DotPitch	11/3/16 2:50 PM	File	C:\Users\GRANDPOOBA...
□	PUP.Optional.DotPitch	11/3/16 2:50 PM	File	C:\Users\GRANDPOOBA...
□	PUP.Optional.DotPitch	11/3/16 2:50 PM	File	C:\Users\GRANDPOOBA...
□	PUP.Optional.DotPitch	11/3/16 2:50 PM	File	C:\Users\GRANDPOOBA...
□	Trojan.MBAMTest	11/3/16 6:19 PM	File	C:\Users\GRANDPOOBA...
□	PUP.Optional.DotPitch	11/3/16 6:19 PM	File	C:\Users\GRANDPOOBA...
□	PUM.Optional.CMDShell	11/3/16 2:50 PM	Registry Value	HKU\S-1-5-21-3106529...

Quarantined items are shown in a table format, with pertinent information presented to help you determine what action needs to be taken. Each item listed has a checkbox in the leftmost column. Check the checkbox to restore or delete the item. Please note that the Restore and Delete buttons are greyed out until items are selected. If you wish to apply the same action to all quarantined items, select the checkbox in the table header and click Restore or Delete.

Please be aware that quarantined items which are not deleted or restored will continue to be visible here until action is taken.

Reports

The Reports Pane displays a list of scans and real-time protection detections, in reverse chronological order. A *Protection Event* that starts with the word *Scan* is a report summarizing the specified scan. All other reports listed on this screen are detail pertaining to detections made by real-time protection. A screenshot is shown here.



Reports

Review scan and protection logs for Malwarebytes. More Information

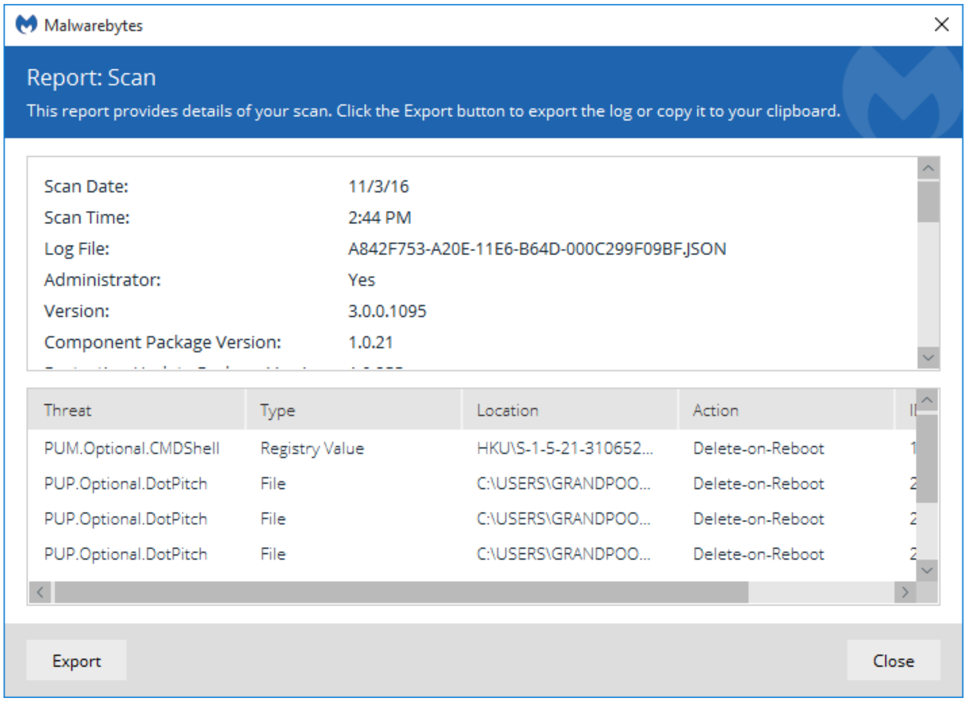
□	Protection Event	Date and Time
□	Scan Report	11/11/16 2:19 PM
□	Scan Report	11/11/16 2:24 PM
□	Scan Report	11/11/16 2:27 PM
□	Scan Report	11/11/16 2:31 PM
□	Scan Report	11/11/16 2:38 PM
□	Website blocked	11/11/16 2:40 PM
□	Website blocked	11/11/16 2:40 PM
□	Website blocked	11/11/16 2:40 PM
□	Website blocked	11/11/16 2:40 PM

Selected reports may be viewed on screen, or exported to a text file for later viewing. Please note that only manual (on demand) scans are available for users of the free version of *Malwarebytes 3*.

- Scan Information
  - **Scan Date:** Date when scan was executed
  - **Scan Time:** Time when scan was completed
  - **Log File:** 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
- Version Information
  - **Version:** *Malwarebytes 3* program version
  - **Component Package Version:** Currently installed version of package that includes various program sub-components
  - **Update Package Version:** Currently installed version of package that includes scanning engine and other related updates
  - **License:** License type (valid values are Free, Premium or Trial)
- System Information
  - **OS:** Operating System version, which also may contain Service Pack information
  - **CPU:** CPU type (valid values are x86 and x64)
  - **File System Type:** File system used on the primary (OS) disk drive (valid values are NTFS, FAT and FAT32)
  - **User:** Windows user name associated with this scan
- 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
    - **Processes:** The number of items detected during the scan
    - **Modules:** The number of items detected during the scan
    - **Registry Keys:** The number of items detected during the scan
    - **Registry Values:** The number of items detected during the scan
    - **Registry Data:** The number of items detected during the scan
    - **Folders:** The number of items detected during the scan
    - **Files:** The number of items detected during the scan
- Object Types/Targets Scanned
    - Eight object types/targets are listed. Each may be enabled (included in scan) or disabled (excluded from scan). These object types are:
        - Memory
        - Startup
        - File System
        - Archives
        - Rootkits
        - Heuristics
        - PUP
        - PUM
- Threats Detected during scan execution, containing the following information:
    - **Threat:** Name of threat, or threat family (as categorized by Malwarebytes Research team)
    - **Type:** Container in which the threat was detected (file, registry key)
    - **Location:** 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 Customer Success if a question arises pertaining to blocking of a specific threat.

The Scan Report may appear in two different forms. If one or more threats were detected during a scan, the report will appear as:



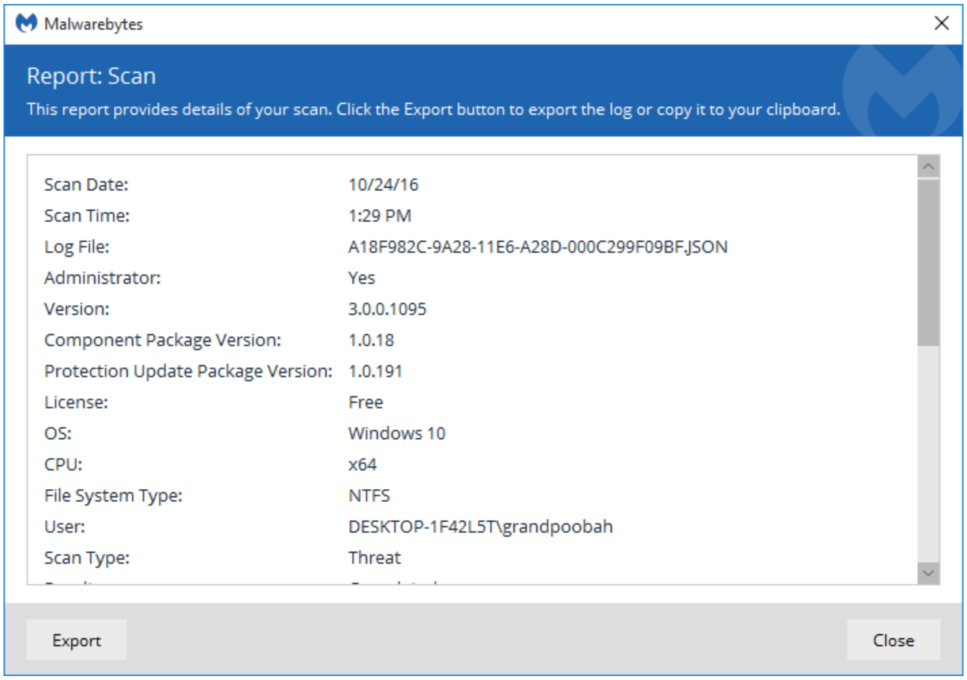
Report: Scan

This report provides details of your scan. Click the Export button to export the log or copy it to your clipboard.

Scan Date:	11/3/16
Scan Time:	2:44 PM
Log File:	A842F753-A20E-11E6-B64D-000C299F09BF.JSON
Administrator:	Yes
Version:	3.0.0.1095
Component Package Version:	1.0.21

Threat	Type	Location	Action
PUM.Optional.CMDShell	Registry Value	HKU\S-1-5-21-310652...	Delete-on-Reboot
PUP.Optional.DotPitch	File	C:\USERS\GRANDPOO...	Delete-on-Reboot
PUP.Optional.DotPitch	File	C:\USERS\GRANDPOO...	Delete-on-Reboot
PUP.Optional.DotPitch	File	C:\USERS\GRANDPOO...	Delete-on-Reboot

Please note that the bottom portion of the report shows the threats detected during the scan. It is scrollable when required. The top portion of the report is a scrollable itemization of the user environment as described above, and shown here:



Report: Scan

This report provides details of your scan. Click the Export button to export the log or copy it to your clipboard.

Scan Date:	10/24/16
Scan Time:	1:29 PM
Log File:	A18F982C-9A28-11E6-A28D-000C299F09BF.JSON
Administrator:	Yes
Version:	3.0.0.1095
Component Package Version:	1.0.18
Protection Update Package Version:	1.0.191
License:	Free
OS:	Windows 10
CPU:	x64
File System Type:	NTFS
User:	DESKTOP-1F42L5T\grandpoobah
Scan Type:	Threat

Viewing or Deleting Logs

You may view any log file by clicking the log to select it, then clicking the View Report button. As mentioned previously, there are several output options for Protection Logs. To delete logs, click the checkbox corresponding to those logs you wish to delete, then click the Delete button. Please bear in mind that computers which have significant threat activity will also have larger logs. You should periodically check how much disk space is being used for logs, so that logs do not impact normal operation of your computer.

Please note that an Export button is shown at the bottom left corner of this screen. This allows you to make a copy of the log for use by other programs. You may export to your clipboard or to a text (TXT) file.

Settings

The Settings screen allows the user to change all operational settings of *Malwarebytes 3*. Using tabs, we have grouped settings by the areas/functions which they control, in order to maintain a clean user interface. When you select any tab, you will see the Detail Pane change to reflect the tab which you selected. At the same time, the tab itself is highlighted.

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

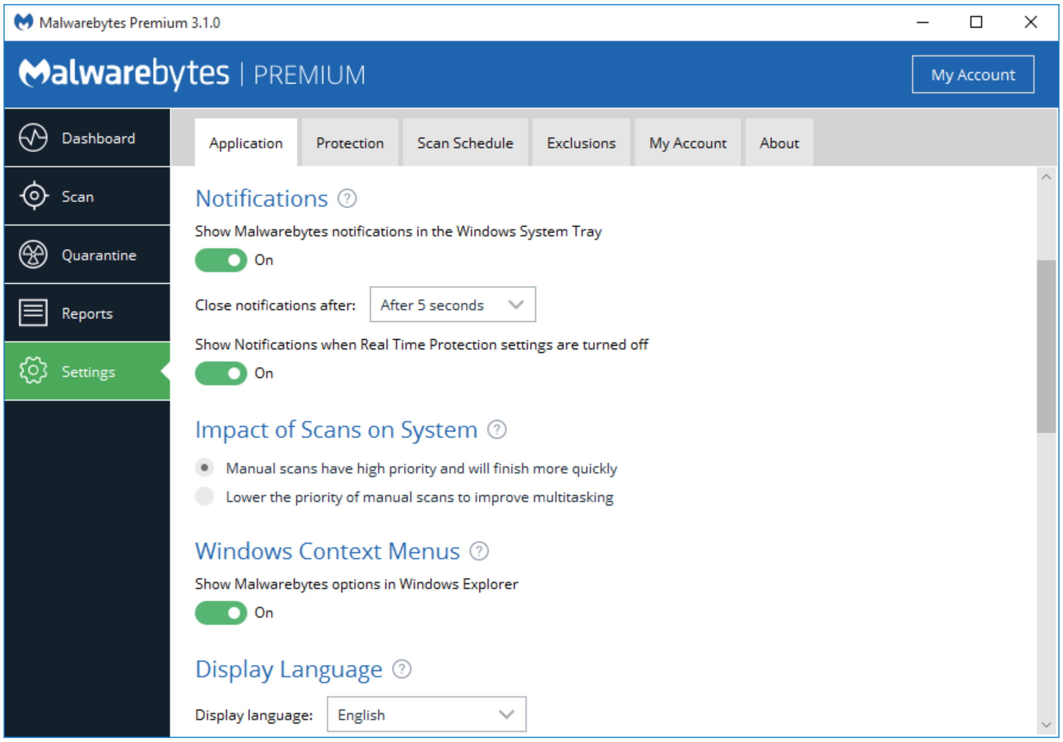
- **Application Settings:** Settings that affect *Malwarebytes 3*, as well as how it coexists with Windows.
- **Protection Settings:** How *Malwarebytes 3* should protect you during scans and (for Premium/Trial mode users only) Real-Time Protection.
- **Scan Schedule:** When *Malwarebytes 3* should execute scans and check for protection updates. This setting is functional only for users of Premium/Trial mode.
- **Exclusions:** Items which will be excluded from testing which detects malware, as well as websites which are categorized as malicious but specifically approved by the user.
- **My Account:** Information pertaining to the status of your subscription.
- **About:** Version numbers corresponding to *Malwarebytes 3* as a whole, and for various components of the program which may be updated individually. Malwarebytes resources are also listed on this page.

When Settings is selected, the *Application* tab is always selected. If you navigate away from Settings – to Dashboard, Scan, Quarantine or Reports – you will always return to the *Application* tab of Settings when you click on Settings.

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

Application Settings

This is the entry screen you will see when you click on Settings in the Menu Pane. It controls how *Malwarebytes 3* interacts with many aspects of your computer's operating system. A screenshot is shown below.



Notifications

Show Malwarebytes notifications in the Windows System Tray: On

Close notifications after: After 5 seconds

Show Notifications when Real Time Protection settings are turned off: On

Impact of Scans on System

● Manual scans have high priority and will finish more quickly

○ Lower the priority of manual scans to improve multitasking

Windows Context Menus

Show Malwarebytes options in Windows Explorer: On

Display Language

Display language: English

The scroll bar at the right of this screen indicates there are many more options available on this screen than what appear here. We will now cover each of them in order.

Application Updates

Malwarebytes 3 may have updates available for individual program components, or for the full program. We provide two toggle switches which allow you to choose whether either or both upgrade modes can be integrated into your copy of *Malwarebytes 3* when they are available. Click Install Application Updates to check for available program updates or upgrades. You can choose if you upgrade, and when. Upgrades only happen with your consent.

Notifications

Notifications regarding scans, real time protection, updates and subscriptions occur in windows at the lower right corner of your screen, outside of the *Malwarebytes 3* interface. You may enable or disable these notifications. Most notifications are enabled by default, while a few can be disabled. **Please note** that some non-critical information may not be visible if you disable notifications. Disabled notifications do not leave the user at risk at any time. The following notifications may be disabled. Please refer to Appendix A (Notification Window Examples) at the end of this guide for further information.

- Malicious Website Blocked
- Malware Detected (auto-quarantine)
- Non-Malware Detected (auto-quarantine)

Some users intentionally turn off one or more components of real-time protection. Users may now disable notifications that components have been turned off. **Please note** that as a result of this setting, users will be unable to receive notifications regarding real-time protection failures in the event of program malfunction.

Impact of Scans on System

Most users schedule scans to occur during times when their computer is typically idle. Execution of a manual scan may be performed as a matter of convenience, or while other tasks are being executed. The performance of lower-powered computers may be affected by execution of the Malwarebytes scan. This setting allows the user to determine the priority of the scan to be performed. Lower scan priority will require more time to execute while impacting other operations to a lesser degree. High priority allows the scan to be executed at the maximum speed which the computer allows, but may affect other tasks.

Windows Context Menus

Malwarebytes 3 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 On.

Display Language

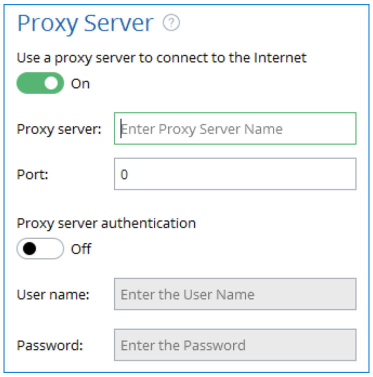
This setting determines the language used throughout. This is pre-set, based on the language used during program installation. It can be modified at will.

Event Log Data

This setting provides additional information regarding program actions which are beyond typical needs of the user. Should you encounter a technical issue with *Malwarebytes 3*, our Customer Success engineers may request that you enable this setting to provide additional troubleshooting information. Once troubleshooting is complete, please remember to turn this setting off to prevent unnecessary disk usage. The default setting is Off.

Proxy Server

This determines whether Internet connections will use a proxy server. This is more often used on a corporate network. It has two primary purposes. The first is to funnel communications to and from the outside world through a single connection point, thus assuring anonymity of all computers on the internal network. The second purpose is to cache content. This means that external content which had recently been downloaded is saved locally for some period of time, and subsequent requests by that user (or others) could use the recently-saved data. This conserves significant bandwidth, resulting in lower operating costs.


Proxy Server

Use a proxy server to connect to the Internet

On

Proxy server: Enter Proxy Server Name

Port: 0

Proxy server authentication

Off

User name: Enter the User Name

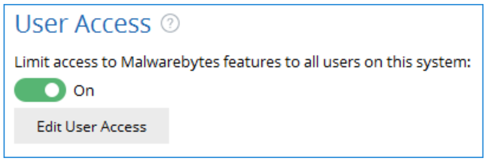
Password: Enter the Password

By default, *Malwarebytes 3* does not use a proxy. If configured to do so, the bottom panel will change to provide configuration options as shown in the screenshot shown here.

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 user name and password which have been assigned to you.

User Access

This slider allows users of *Malwarebytes 3* Premium and *Malwarebytes 3* Premium Trial versions to restrict access to various features and functions in *Malwarebytes 3* with password protection. The Edit User Access button is only visible when the slider is in the **On** position, allowing the user to define sections of the program which require a password to access.

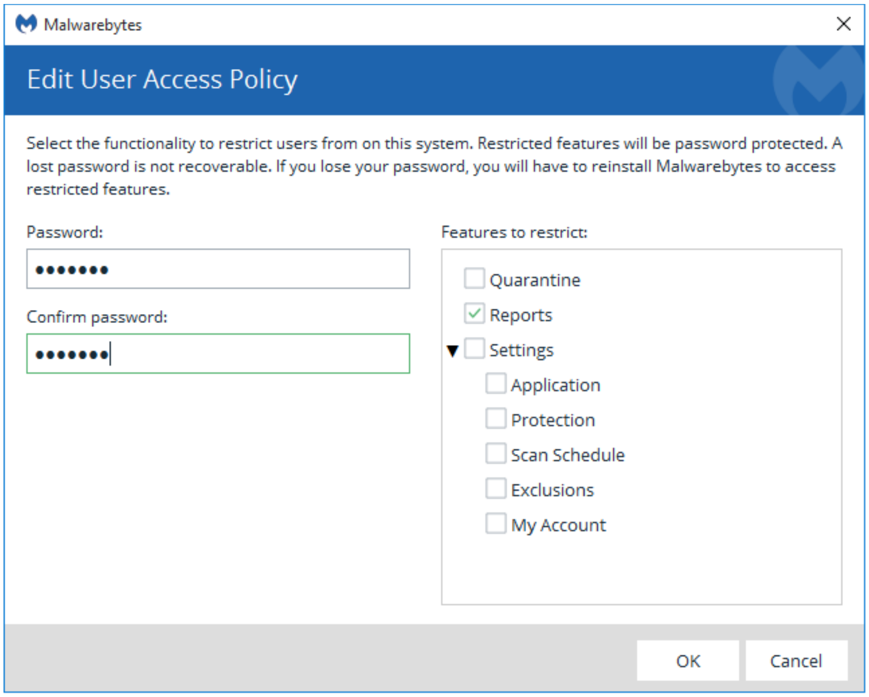

User Access

Limit access to Malwarebytes features to all users on this system:

On

When the Edit User Access button is clicked, a new window opens directly above the *Malwarebytes 3* program screen to restrict access to selected areas of the program only to those users who possess the password. The password is also defined on this screen.

WARNING: This password is not recoverable. If you lose your password, you will have to reinstall *Malwarebytes 3* to access restricted features.


Malwarebytes

Edit User Access Policy

Select the functionality to restrict users from on this system. Restricted features will be password protected. A lost password is not recoverable. If you lose your password, you will have to reinstall Malwarebytes to access restricted features.

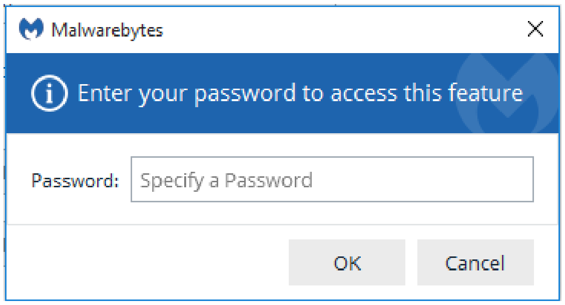
Password: •••••••

Confirm password: •••••••

Features to restrict:

- ☐ Quarantine
- ☑ Reports
- ☐ Settings
  - ☐ Application
  - ☐ Protection
  - ☐ Scan Schedule
  - ☐ Exclusions
  - ☐ My Account

As shown above, the Reports tab has been placed under password control. This also causes User Access to be placed under password control. This prevents unauthorized users from gaining access to restricted areas.

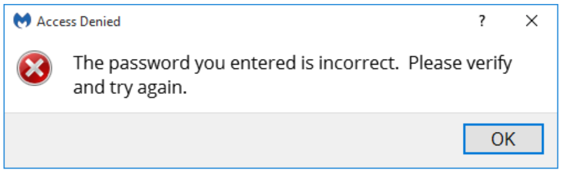


Malwarebytes

Enter your password to access this feature

Password: Specify a Password

When attempting to gain access to a restricted area, you will be required to enter a password (as shown here).



Access Denied

The password you entered is incorrect. Please verify and try again.

If an incorrect password is entered, or if a null password is used, this error message will be displayed.

If this feature has been enabled and is subsequently disabled, any restrictions which have been defined are cancelled. This feature is not available to users of the Free version. Currently, only one policy may be in effect at any given time.

Windows Action Center

You may have noticed an icon in your system tray with a red X superimposed over an white flag. That is a status indicator for the Windows Action Center, which tells you when your computer has a security issue that needs your attention. *Malwarebytes Premium 3* or *Malwarebytes Premium Trial 3* can now be registered as a security solution on your computer. There are three settings available, which will be abbreviated here for easier reading. Brief descriptions for the meaning of each setting are also provided.

- **Let Malwarebytes choose whether to register:** *Malwarebytes 3* will determine whether it should be registered in Action Center. The program will not register when Microsoft Security Essentials is in use on a Windows 7 or older operating system. It will also not register when Windows Defender is used on a Windows 8 or newer OS.
- **Always register Malwarebytes:** *Malwarebytes 3* program status will always appear in Action Center.
- **Never register Malwarebytes:** *Malwarebytes 3* program status will never appear in Action Center.

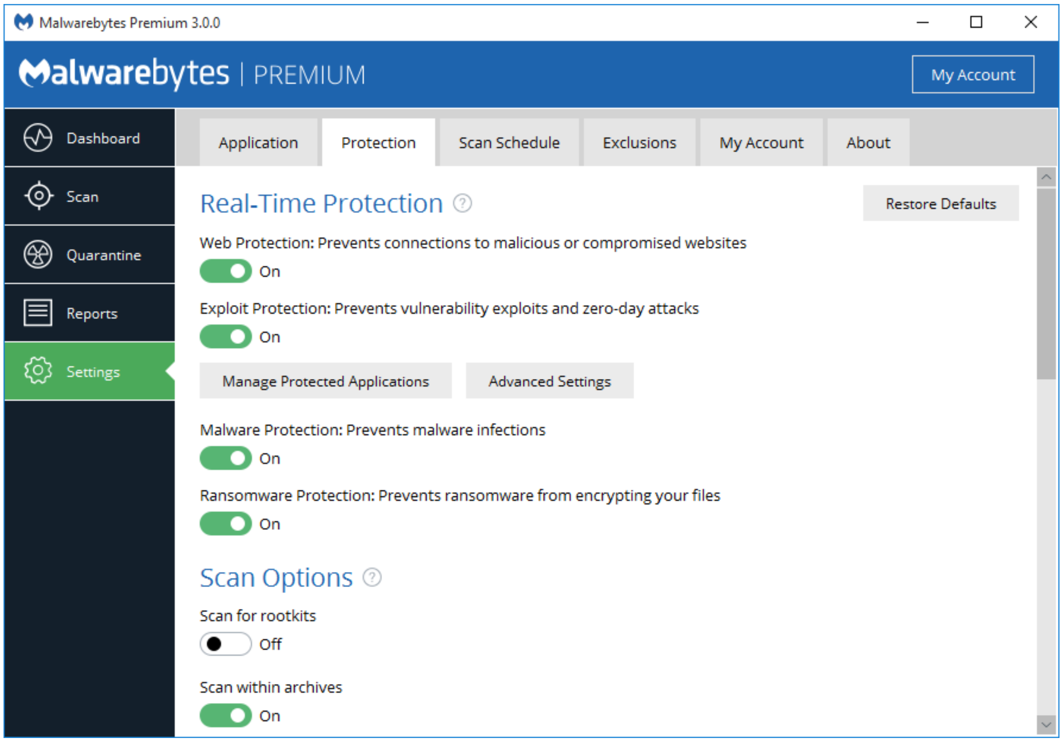
Usage and Threat Statistics

If you check this box, you will be sending us information that helps us do our jobs. We like to know what countries *Malwarebytes 3* is being used in, and the breakdown of subscriptions, Trial versions, 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. We hope that's fine with you as well. For a full list of information that is collected, please see the Malwarebytes Privacy Policy, at:

https://www.malwarebytes.com/privacy/

Protection

Most settings which control how *Malwarebytes 3* protects your computer are located on the Protection tab. Settings are grouped by category. A screenshot is shown below, along with descriptions of all settings available on this tab.



Real-Time Protection

Web Protection: Prevents connections to malicious or compromised websites
On

Exploit Protection: Prevents vulnerability exploits and zero-day attacks
On

Malware Protection: Prevents malware infections
On

Ransomware Protection: Prevents ransomware from encrypting your files
On

Scan Options

Scan for rootkits
Off

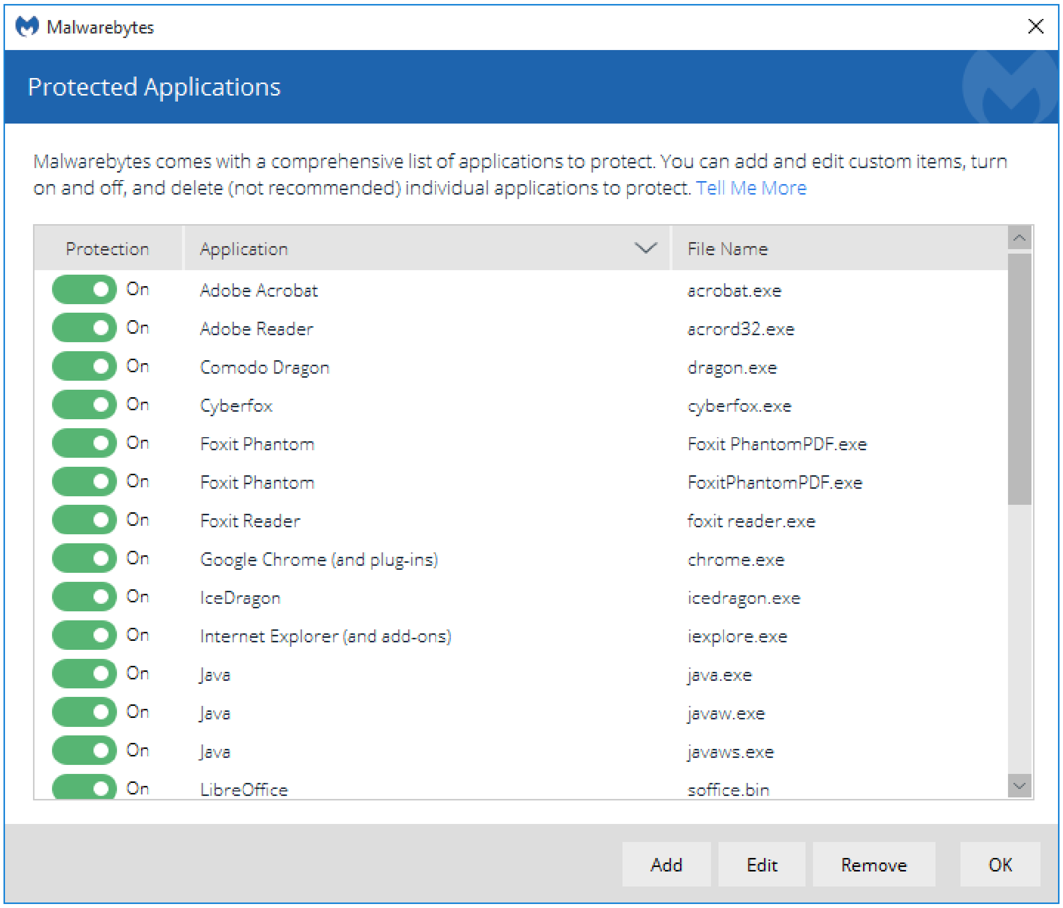
Scan within archives
On

Real-Time Protection

Malwarebytes 3 offers four different types of real-time protection. These features are available only to users of the Premium and Trial modes. It is important to note that Trial users who do not convert to a Premium subscription will lose all real-time protection features at the end of their trial.

Web Protection protects Premium/Trial users by blocking access to/from Internet addresses which are known or suspected of engaging in malicious activity. This feature 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 this option is disabled if you are using the Free version.

Exploit Protection uses multiple protection layers to guard against attempted exploits of vulnerabilities in legitimate applications. When applications are launched by the user, exploit protection is also launched as a shield. This protection will often detect and neutralize attacks that go undetected by other security applications. It is on by default for Premium/Trial users.

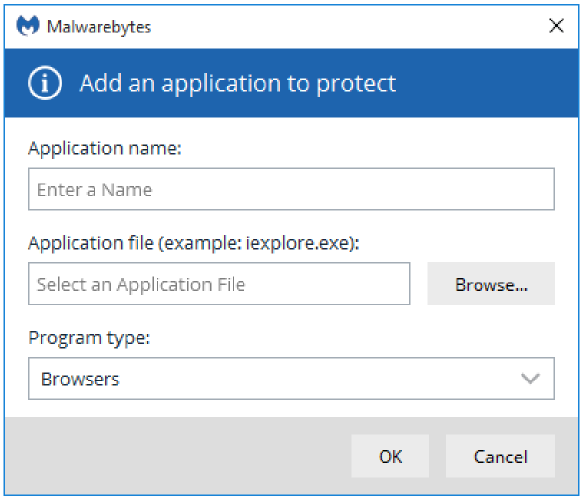


Protected Applications

Malwarebytes comes with a comprehensive list of applications to protect. You can add and edit custom items, turn on and off, and delete (not recommended) individual applications to protect. Tell Me More

Protection	Application	File Name
On	Adobe Acrobat	acrobat.exe
On	Adobe Reader	acrord32.exe
On	Comodo Dragon	dragon.exe
On	Cyberfox	cyberfox.exe
On	Foxit Phantom	Foxit PhantomPDF.exe
On	Foxit Phantom	FoxitPhantomPDF.exe
On	Foxit Reader	foxit reader.exe
On	Google Chrome (and plug-ins)	chrome.exe
On	IceDragon	icedragon.exe
On	Internet Explorer (and add-ons)	iexplore.exe
On	Java	java.exe
On	Java	javaw.exe
On	Java	javaws.exe
On	LibreOffice	soffice.bin

Many popular applications have been pre-configured for shielding. A screenshot is shown above. To change the status of any application, either use the Protection slider, or double click either the Application or File Name. Premium/Trial users may add protection for other applications, and edit specifications for any defined shield. The Edit screen is shown here.



Add an application to protect

Application name:

Enter a Name

Application file (example: iexplore.exe):

Select an Application File

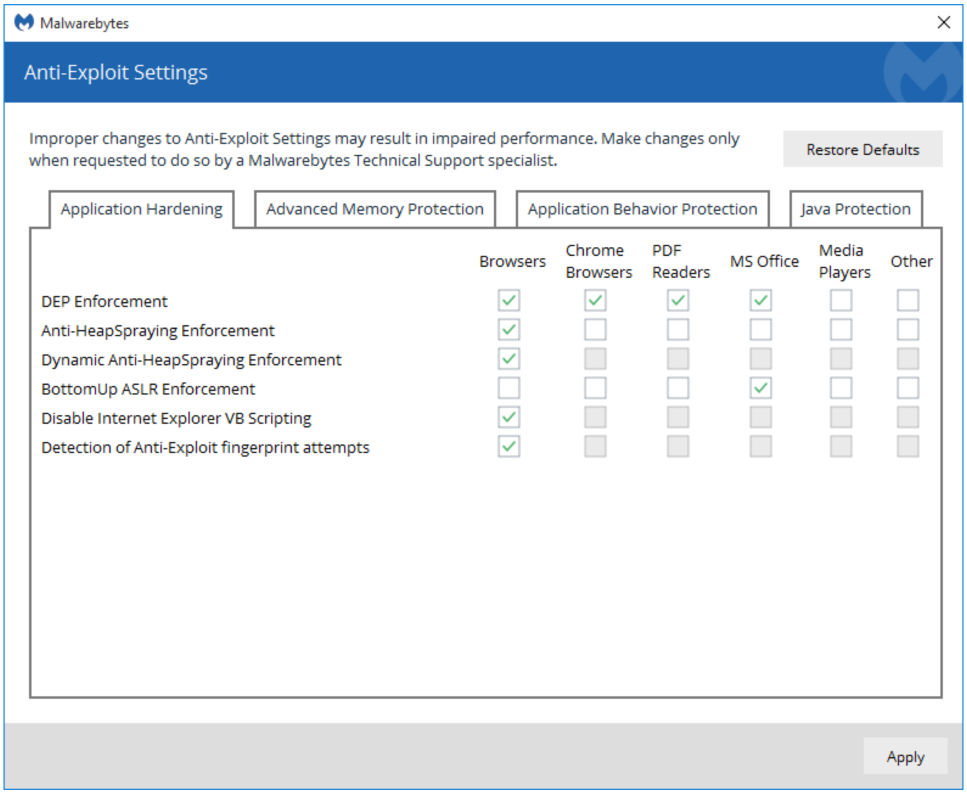
Program type:

Browsers

You may specify an Application name which is easily recognizable, and the Application file name. You can also browse for the file. Select a Program type which most closely resembles the purpose of the application. If you are unsure, select **Other**.

The same screen is used to edit existing entries.

In addition, Premium/Trial users can modify advanced exploit protection settings. Several advanced settings are spread across four tabs, depending on the classification of protection they provide. One tab is shown here as an example.



Improper changes to Anti-Exploit Settings may result in impaired performance. Make changes only when requested to do so by a Malwarebytes Technical Support specialist.

	Browsers	Chrome Browsers	PDF Readers	MS Office	Media Players	Other
DEP Enforcement	☑	☑	☑	☑	☐	☐
Anti-HeapSpraying Enforcement	☑	☐	☐	☐	☐	☐
Dynamic Anti-HeapSpraying Enforcement	☑	▨	▨	▨	▨	▨
BottomUp ASLR Enforcement	☐	☐	☐	☑	☐	☐
Disable Internet Explorer VB Scripting	☑	▨	▨	▨	▨	▨
Detection of Anti-Exploit fingerprint attempts	☑	▨	▨	▨	▨	▨

Each advanced setting is available for up to six different application groups, the groups representing the method by which threats will attempt to exploit vulnerabilities in applications of that type. Protection may be turned on (checked), off (unchecked), or is not applicable for that group of applications (greyed out). While these settings provide very specific protection, they should only be changed when requested by a Malwarebytes Customer Success specialist. Incorrect settings may result in impaired protection.

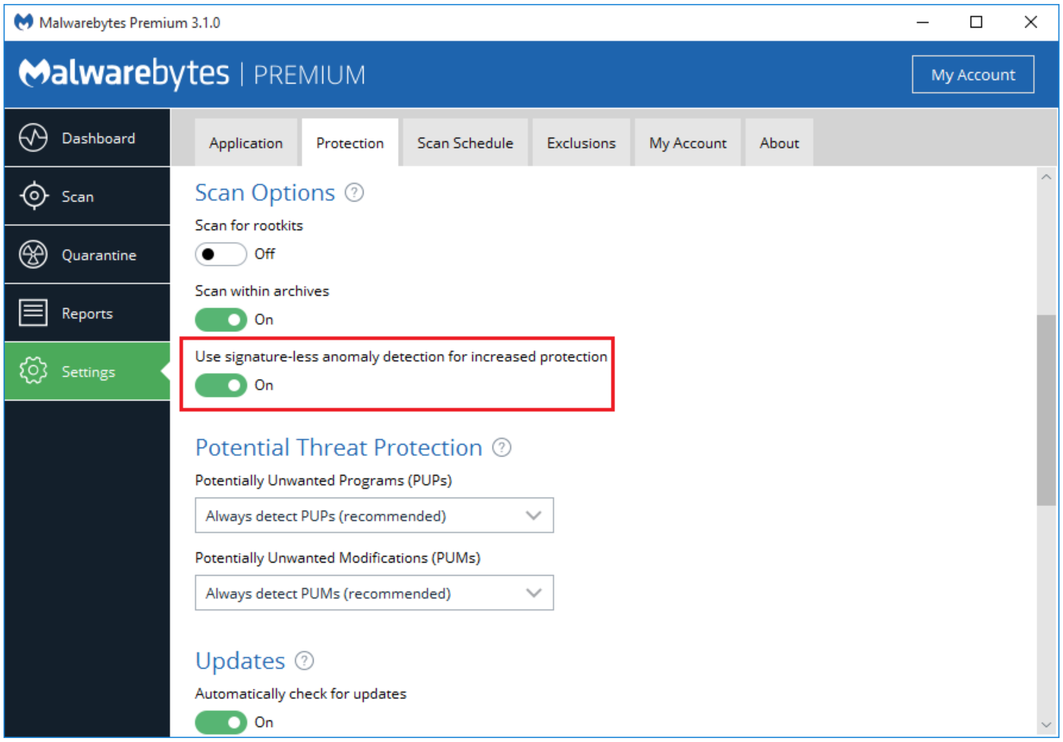
Malware Protection may be turned on or off as needed by Premium/Trial users. It is on by default. This feature protects against malware present in code/files that try to execute on your computer. These files may have been downloaded, imported from a USB drive, or received as an email attachment. While we do not recommend disabling this protection mechanism, there may be times when it needs to be done to troubleshoot compatibility issues that arise with anti-virus updates or computer startup problems. If either situation does occur, start your computer in Safe Mode, disable Malware Protection, isolate and correct the issue, then turn Malware Protection back on. **Please note** that this option is disabled if you are using the Free version.

Ransomware Protection provides Premium/Trial users protection against the threat of ransomware. This protection is not available for users of Windows XP or Windows Vista. While all other protection features may provide some degree of protection against ransomware, well-crafted ransomware may go undetected until it attempts to initiate its attack. As many computer users have found, there is little or no remedy available after the fact. We strongly recommend that ransomware protection be turned on at all times. It is on by default. **Please note** that this option is disabled if you are using the Free version.

Scan Options

Scan for rootkits utilizes a specific set of rules and tests to determine if a rootkit is present on your computer. For readers who are unfamiliar with this term, an explanation may be handy. A rootkit is malicious software that can be placed on a computer which has the ability to 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 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 3* will scan four levels deep within archive (ZIP, RAR, 7Z, CAB and MSI) files. If this option is disabled, the archive is excluded from scanning. **Please note** that encrypted archives cannot be fully tested.



Scan Options

Scan for rootkits
Off

Scan within archives
On

Use signature-less anomaly detection for increased protection
On

Potential Threat Protection

Potentially Unwanted Programs (PUPs)
Always detect PUPs (recommended)

Potentially Unwanted Modifications (PUMs)
Always detect PUMs (recommended)

Updates

Automatically check for updates
On

We have introduced a new detection method called *Shuriken 2.0*, a signature-less technology. *Shuriken* takes advantage of machine learning to supplement existing detection methods, and does introduce a slight performance penalty.

Potential Threats

In addition to malicious software detection and elimination, *Malwarebytes 3* 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. These are:

- **Ignore detections:** *Malwarebytes 3* will not act on detection, nor will you be alerted.
- **Warn user:** You will be alerted to the detection. You may choose to ignore it, create an exclusion, or treat it as malware.
- **Always detect PUPs/PUMs (recommended):** 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.

Updates

Users of *Malwarebytes Premium 3* and *Malwarebytes Premium Trial 3* have the ability to automatically check for protection updates, and to specify when those checks will be performed. The date range is adjustable between fifteen (15) minutes and fourteen (14) days, the increment depending on the range (minutes/hours/days). We recommend that you do not allow the rules database to become dated, as much damage can be caused by zero-day infections – those threats that are too new to be adequately protected against by anti-virus software. The default for this feature is on. You may also have *Malwarebytes 3* display a notification in the corner of your screen if protection updates are more than 24 hours old.

Startup Options

These settings define how *Malwarebytes 3* behaves when your computer starts. You may launch several applications at startup, and they may initiate processes which require *Malwarebytes 3* launch timing to be adjusted. Let's look at each setting in detail.

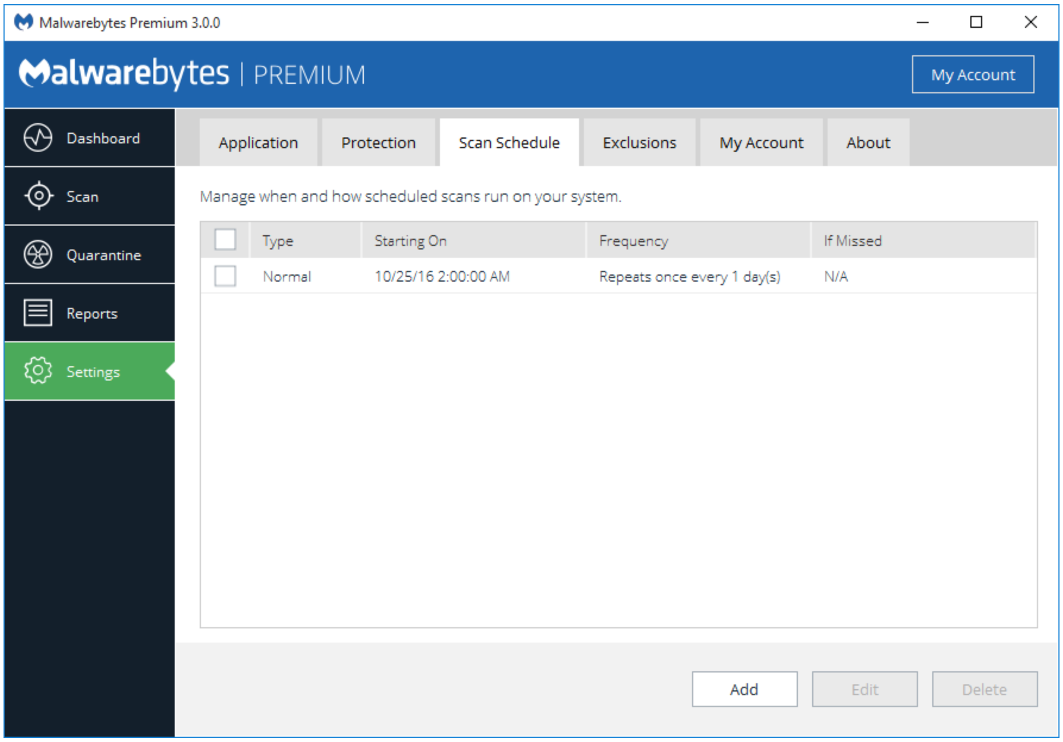
- **Start Malwarebytes at Windows startup:** If this setting is unchecked, *Malwarebytes 3* will not start with Windows. No real-time protection layers will start when Windows starts, though they may still be started manually by launching *Malwarebytes 3*.
- **Delay Real-Time Protection when Malwarebytes starts:** There may be times when the startup of system services used by *Malwarebytes 3* conflicts with services required by other applications at boot time. When this is the case, turn this setting on. You may also adjust the delay timing. You will need to experiment with the specific delay setting necessary to compensate for any conflicts that are noted. 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.
- **Enable self-protection module:** This setting controls whether *Malwarebytes 3* creates a *safe zone* to prevent malicious manipulation of the program and its components. Checking this box introduces a one-time 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 module early start:** When self-protection 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.

Quarantine

Users of *Malwarebytes Premium 3* and *Malwarebytes Premium Trial 3* may specify whether malware will be automatically quarantined when it is detected. The default setting is on. If the users declines to automatically quarantine malware, a notification will display in the lower right corner of the screen for each detection, and the user must specify whether the file is to be ignored once, ignored always (added to Exclusions) or quarantined.

Scan Schedule

This tab allows users of the Premium and Trial versions to add, edit and remove scheduled scans to be executed by *Malwarebytes 3*. This feature is not available to users of the Free version. A screenshot of this tab is shown below.



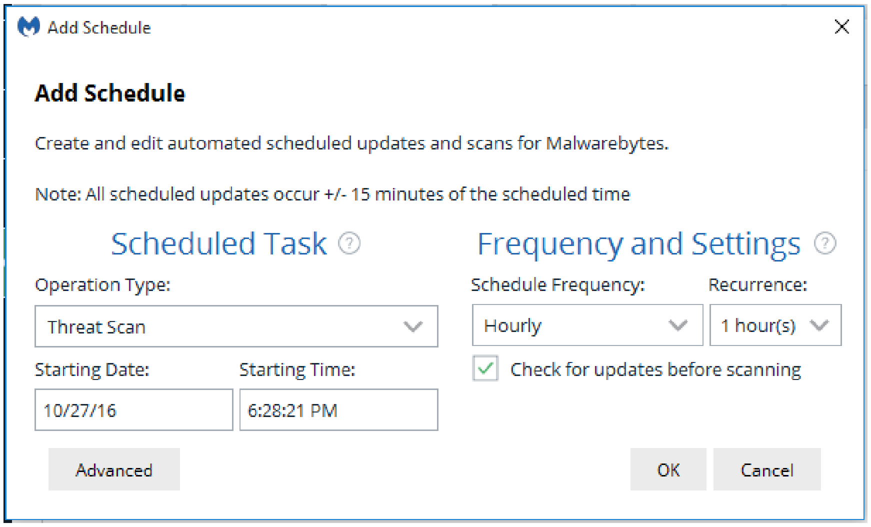
Manage when and how scheduled scans run on your system.

□	Type	Starting On	Frequency	If Missed
□	Normal	10/25/16 2:00:00 AM	Repeats once every 1 day(s)	N/A

One scan is defined when *Malwarebytes 3* is installed. You are free to modify or delete scans at will. **<u>Please note</u>** that if the task is deleted without a replacement task being defined, your *Malwarebytes 3* 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.

Basic Mode

A screenshot of the basic <u>Add Schedule</u> screen is shown here.



Add Schedule

Create and edit automated scheduled updates and scans for Malwarebytes.

Note: All scheduled updates occur +/- 15 minutes of the scheduled time

Scheduled Task

Operation Type: Threat Scan

Starting Date: 10/27/16

Starting Time: 6:28:21 PM

Frequency and Settings

Schedule Frequency: Hourly

Recurrence: 1 hour(s)

☑ Check for updates before scanning

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:

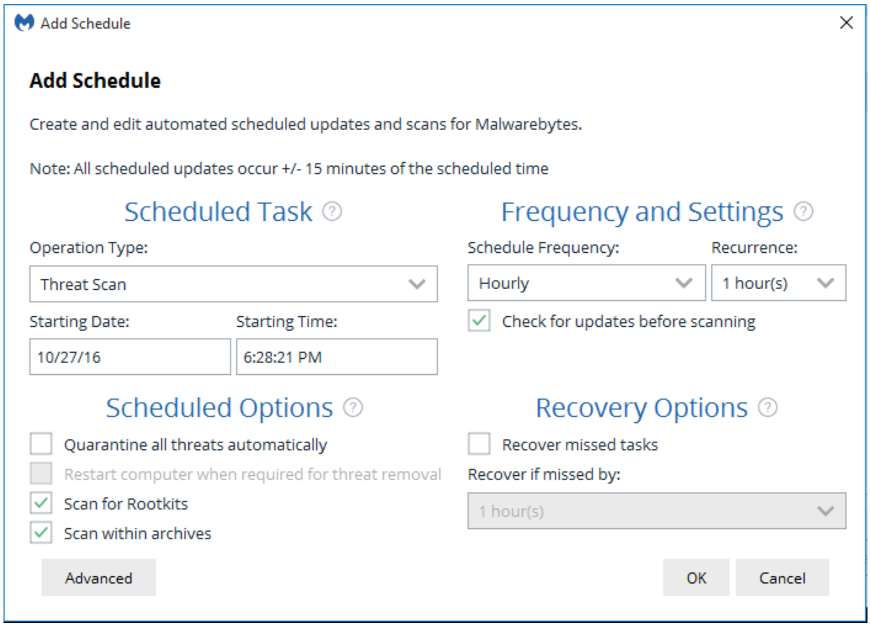
- Threat Scan
- Custom Scan
- Hyper Scan

Scan types have been previously discussed in the Scan section of this guide (pages 11-13). Please refer to those pages 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

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.



Add Schedule

Add Schedule

Create and edit automated scheduled updates and scans for Malwarebytes.

Note: All scheduled updates occur +/- 15 minutes of the scheduled time

Scheduled Task

Operation Type: Threat Scan

Starting Date: 10/27/16

Starting Time: 6:28:21 PM

Frequency and Settings

Schedule Frequency: Hourly

Recurrence: 1 hour(s)

☑ Check for updates before scanning

Scheduled Options

☐ Quarantine all threats automatically

☐ Restart computer when required for threat removal

☑ Scan for Rootkits

☑ Scan within archives

Recovery Options

☐ Recover missed tasks

Recover if missed by: 1 hour(s)

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.

Advanced Scan Options

Scheduled Task defines what task (scan/update) is to be added/edited, and when that task should begin – specifying both the date and time. Schedule Options provides several added capabilities to the basic settings which have already been described. Here's a rundown on the advanced options.

- **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 Customer Success will assist you in having the offending file evaluated more fully by our Research group.

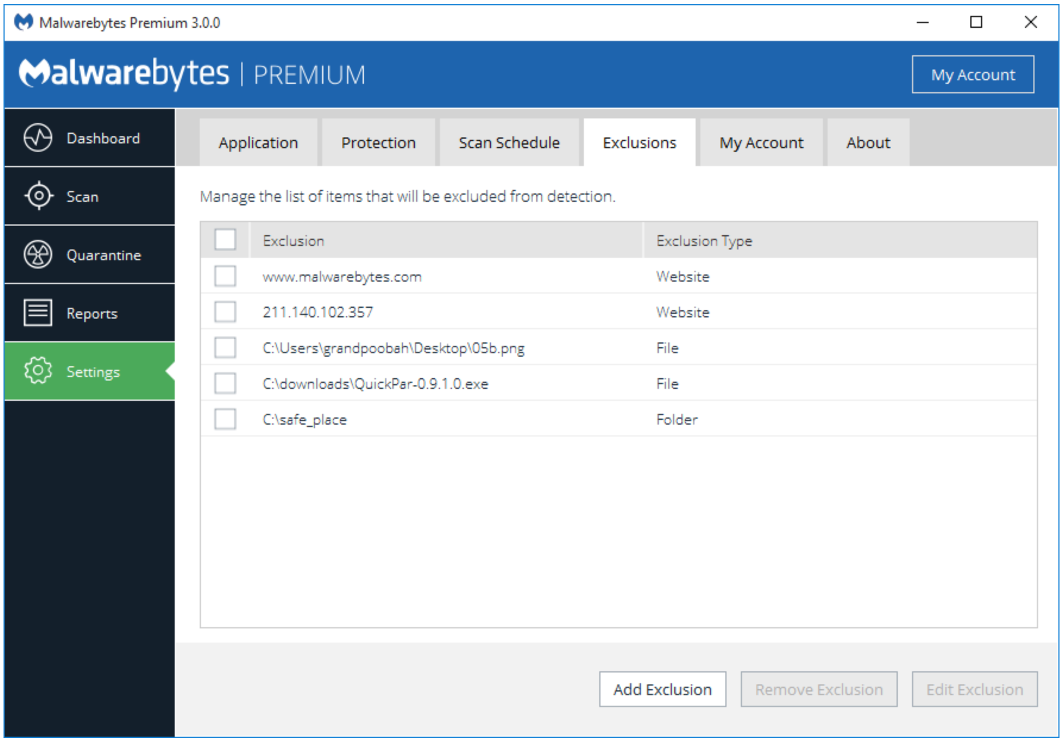
- **Restart computer when required for threat removal:** This is available only if threats are automatically quarantined, and is not selected by default. Some threats may require a computer restart to completely eliminate the threat, but we feel it's best to notify you at the time, so you may save your 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. This option is not available for Hyper Scans.
- **Scan within archives:** This is selected by default. It allows scanning to go four levels deep within archive files. If this setting is not selected, the archive will be ignored. It will also be ignored if it is encrypted. This option is not available for Hyper Scans.

Frequency and Settings was discussed in the previous section (*Advanced Mode*). Please refer to that section for more detail.

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). A scheduled task – if missed – will run at its next opportunity as long as it is within the duration specified by the **Recover if missed by** selector and the **Recover missed tasks** checkbox is checked.

Exclusions

This tab allows additions to, or deletions from a list of items to be excluded from scans. The list may include files, folders, websites, applications which connect to the Internet, or previously detected exploits. A screenshot is shown below.

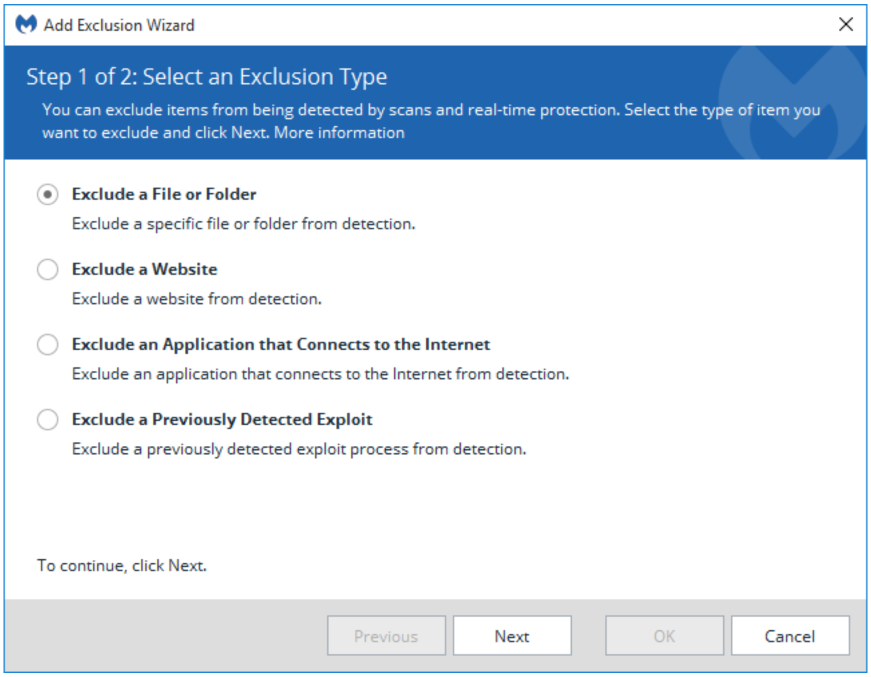


Manage the list of items that will be excluded from detection.

☐	Exclusion	Exclusion Type
☐	www.malwarebytes.com	Website
☐	211.140.102.357	Website
☐	C:\Users\grandpoobah\Desktop\05b.png	File
☐	C:\downloads\QuickPar-0.9.1.0.exe	File
☐	C:\safe_place	Folder

Add Exclusion

Exclusions are items which are exempt from scanning and from real-time protection. The list of items includes files, folders, web sites, applications and safe programs which have been identified as exploits. Clicking the Add Exclusion button launches the Add Exclusion Wizard, as shown below.


Add Exclusion Wizard

Step 1 of 2: Select an Exclusion Type

You can exclude items from being detected by scans and real-time protection. Select the type of item you want to exclude and click Next. More information

● **Exclude a File or Folder**
Exclude a specific file or folder from detection.

○ **Exclude a Website**
Exclude a website from detection.

○ **Exclude an Application that Connects to the Internet**
Exclude an application that connects to the Internet from detection.

○ **Exclude a Previously Detected Exploit**
Exclude a previously detected exploit process from detection.

To continue, click Next.

You may then add items – one at a time – to the list of exclusions. Each item type is defined by criteria as follows:

- **File or folder:** Its location on the file system, and whether it should be excluded from malware *and* ransomware, only malware or only ransomware. 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 3* 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 is commonly offered by anti-virus vendors as well.

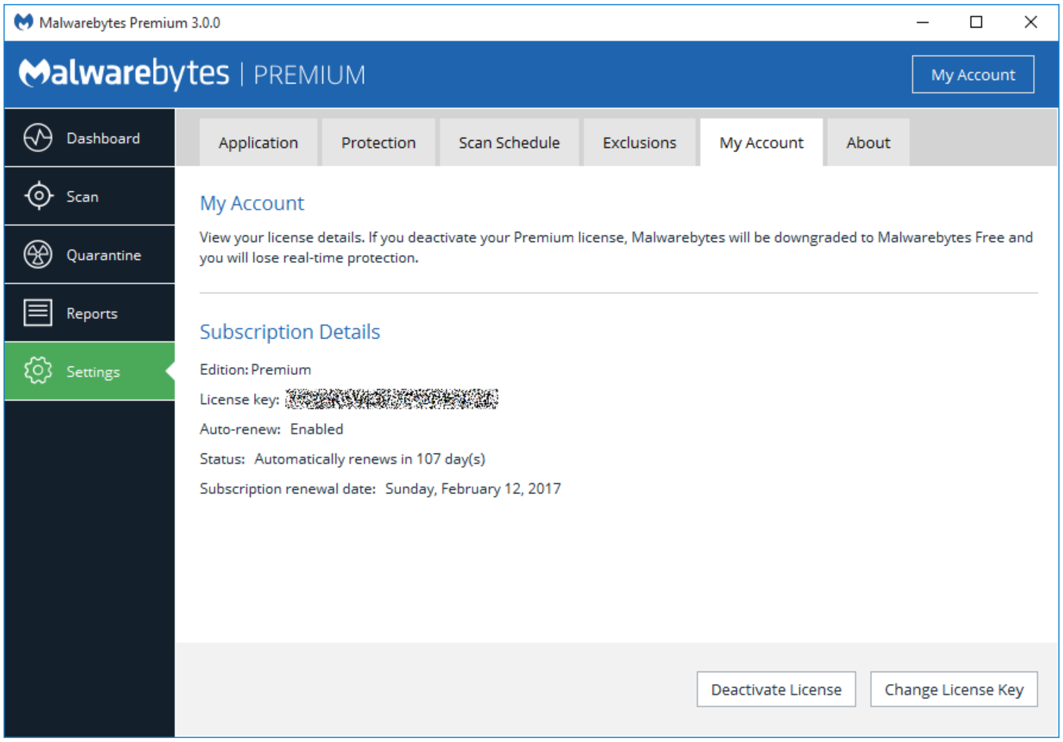
NOTES:

- Clicking **Select Folder…** selects **only** folders, which by default will also exclude any files within those folders, as well as subfolders.
- Clicking **Select Files…** selects individual files for exclusion. The status of the folder is unchanged.

- **Website:** Enter the Domain or IP Address to specify the web address. When adding a domain manually, please 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. Also, domain exclusions are only functional on Windows Vista Service Pack 2, Windows 7, Windows 8.x and Windows 10. **Please note:** Exclusions can also be added by clicking the link in the notification message when the website is blocked by Malwarebytes Website Protection.
- **Application that connects to the Internet:** Specify the name of the application. This is most applicable if the detection is a false positive (legitimate application with some similar characteristics to malware).
- **Previously Detected Exploit:** Specify the MD5 hash of the exploit. This is most applicable if the detection is a false positive (legitimate application with some similar characteristics to malware). The hash guarantees uniqueness of the file in question.

My Account

This tab displays the status of your account, and provides options for you to deactivate your license – useful when moving your Malwarebytes program to a new computer – or change license key. A screenshot is shown below.



My Account

View your license details. If you deactivate your Premium license, Malwarebytes will be downgraded to Malwarebytes Free and you will lose real-time protection.

Subscription Details

Edition: Premium

License key: [redacted]

Auto-renew: Enabled

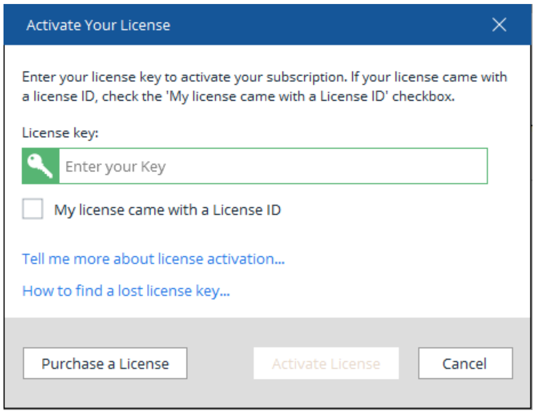
Status: Automatically renews in 107 day(s)

Subscription renewal date: Sunday, February 12, 2017

All of the information shown here is self-explanatory. A set of option buttons are available at the bottom of the screen. The options vary depend on the mode of the program. Buttons for the three program modes are shown below.

Premium Mode options	Deactivate License Change License Key
Trial Mode options	Deactivate Premium Trial I Already Have a License Upgrade Now
Free mode options	I Already Have a License Upgrade Now
Free mode Options (*)	I Already Have a License Start My Premium Trial Upgrade Now

When *Malwarebytes 3* was installed, Premium Trial mode was set automatically (if you were eligible for a trial). There may be circumstances where you have the option of re-entering Trial mode. This would result in the second Free mode display. If you click the button **Change License Key** (Premium mode) or **I Already Have a License** (Trial or Free mode), you will see the following screen superimposed over the *Malwarebytes 3* interface.



Enter your license key to activate your subscription. If your license came with a license ID, check the 'My license came with a License ID' checkbox.

License key: Enter your Key

□ My license came with a License ID

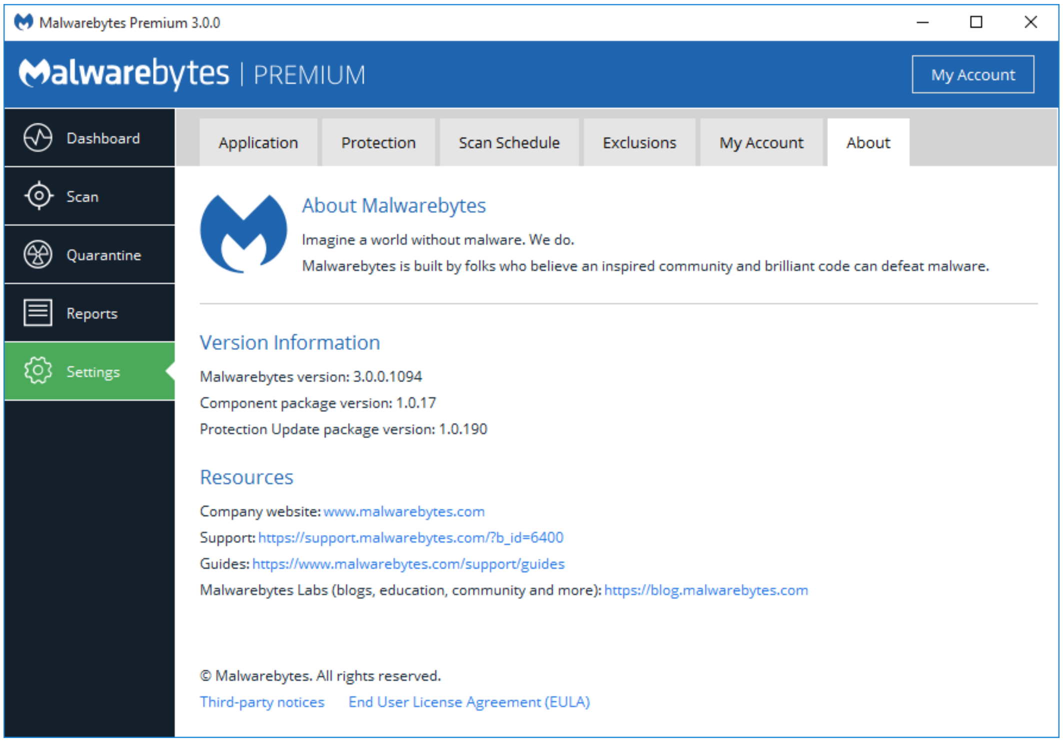
Tell me more about license activation...

How to find a lost license key...

Follow screen instructions to enter your license information. If you do not have a license, either press **Cancel** (to close this window and return to the screen you came from), or **Purchase a License** to go to the Malwarebytes website and purchase a license for the product.

About

This tab tells you more about *Malwarebytes 3*, and what resources are available to you should you need technical assistance. A screenshot is shown below.



About Malwarebytes

Imagine a world without malware. We do.

Malwarebytes is built by folks who believe an inspired community and brilliant code can defeat malware.

Version Information

Malwarebytes version: 3.0.0.1094

Component package version: 1.0.17

Protection Update package version: 1.0.190

Resources

Company website: www.malwarebytes.com

Support: https://support.malwarebytes.com/?b_id=6400

Guides: https://www.malwarebytes.com/support/guides

Malwarebytes Labs (blogs, education, community and more): https://blog.malwarebytes.com

© Malwarebytes. All rights reserved.

Third-party notices   End User License Agreement (EULA)

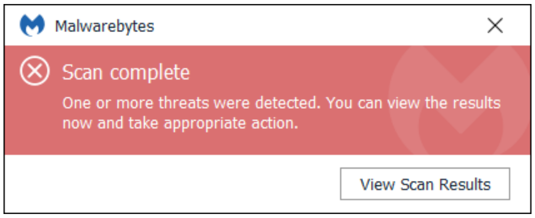
The upper panel contains Version Information. We have split up the program into software components. If you have configured the program to provide program updates, it is easier and faster for us to provide the newest version to you by updating the components that have changed, rather than updating the entire program. It also benefits you if you need technical support, because the versions of each component may influence the direction that our Customer Success engineers take when troubleshooting an issue.

The Resources section provides contact addresses (URLs) which may assist you for sales, support, and educational purposes. In addition, you can view the third-party notices (open source software which we use in our products) as well as a link to our End User Licensing Agreement (EULA).

Appendix A: Notification Window Examples

Malwarebytes 3 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 *Application Settings* (page 23).

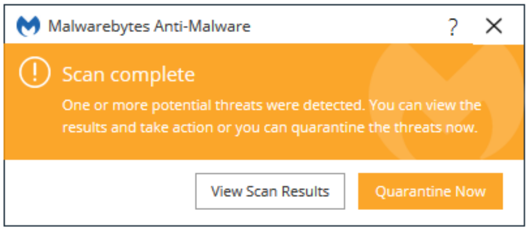
Scan Notifications



Scan complete

One or more threats were detected. You can view the results now and take appropriate action.

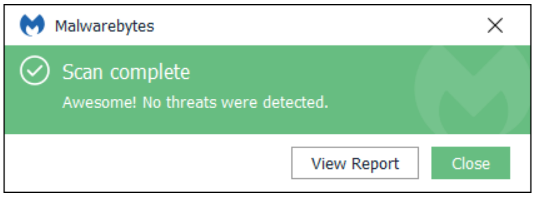
A scan (scheduled or on-demand) has been completed. Malware was detected during execution of the scan. Click the View Scan Results button to review the scan log to determine the exact nature of the threat(s).



Scan complete

One or more potential threats were detected. You can view the results and take action or you can quarantine the threats now.

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. Click the View Scan Results button to review the scan log to determine the exact nature of the threat(s).

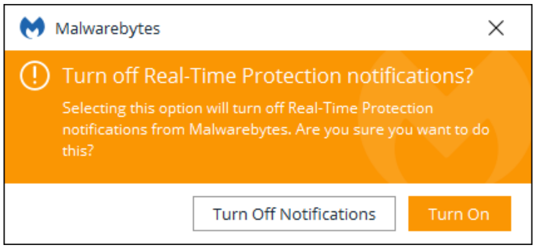


Scan complete

Awesome! No threats were detected.

A scan (scheduled or on demand) has been completed. No problems were detected.

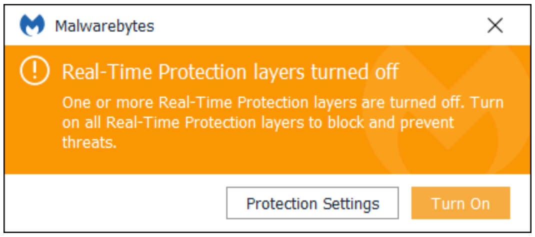
Real Time Protection Notifications



Turn off Real-Time Protection notifications?

Selecting this option will turn off Real-Time Protection notifications from Malwarebytes. Are you sure you want to do this?

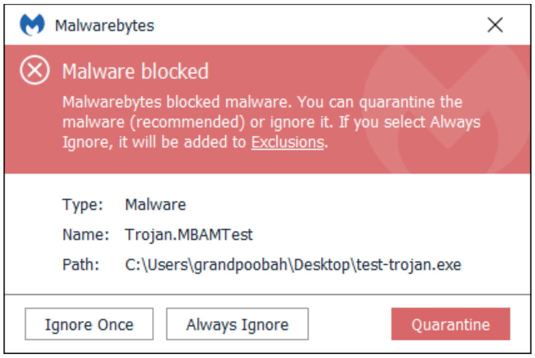
After the user has indicated that they wish to turn off notifications regarding real-time protection components, this notification will be displayed to request confirmation of the user's wishes.



Real-Time Protection layers turned off

One or more Real-Time Protection layers are turned off. Turn on all Real-Time Protection layers to block and prevent threats.

One or more components of real-time protection are disabled. You may re-enable protection by clicking the Turn On button, or by clicking the Protection Settings button. This is not available for *Malwarebytes 3* free users.

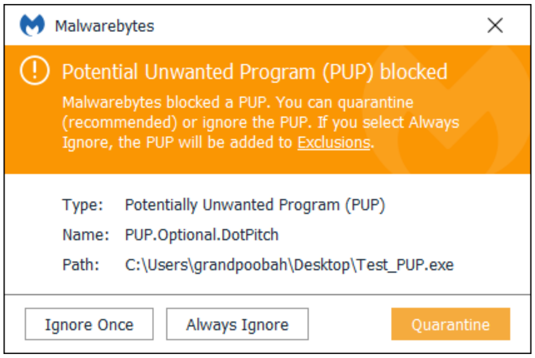


Malware blocked

Malwarebytes blocked malware. You can quarantine the malware (recommended) or ignore it. If you select Always Ignore, it will be added to Exclusions.

Type: Malware
Name: Trojan.MBAMTest
Path: C:\Users\grandpoobah\Desktop\test-trojan.exe

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 execution once, always, or elect to quarantine it at this time. This is not available for *Malwarebytes Free 3* users.

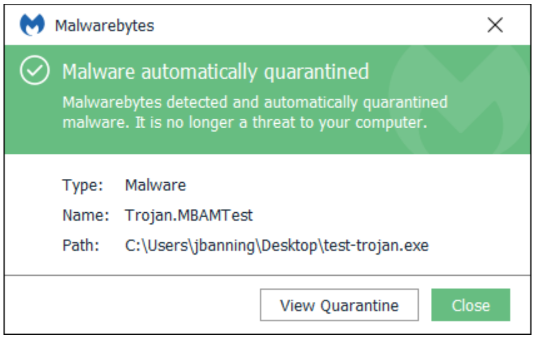


Potential Unwanted Program (PUP) blocked

Malwarebytes blocked a PUP. You can quarantine (recommended) or ignore the PUP. If you select Always Ignore, the PUP will be added to Exclusions.

Type: Potentially Unwanted Program (PUP)
Name: PUP.Optional.DotPitch
Path: C:\Users\grandpoobah\Desktop\Test_PUP.exe

Real-time protection has detected a Potentially Unwanted Program (PUP). You have not chosen to ignore this type of activity, or to exercise the auto-quarantine capability upon detection, so no specific action has been taken. This detection may be acceptable to you, so you may choose to ignore it once, always, or elect to quarantine it at this time. This is not available for *Malwarebytes Free 3* users.

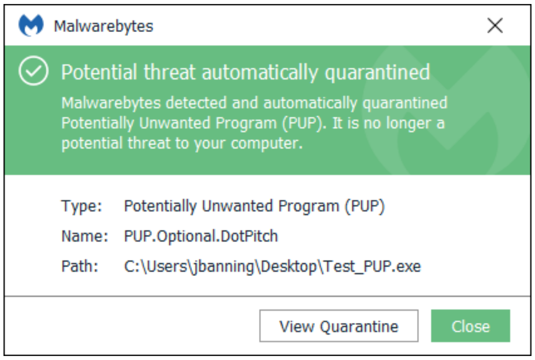


Malware automatically quarantined

Malwarebytes detected and automatically quarantined malware. It is no longer a threat to your computer.

Type: Malware
Name: Trojan.MBAMTest
Path: C:\Users\jbanning\Desktop\test-trojan.exe

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.

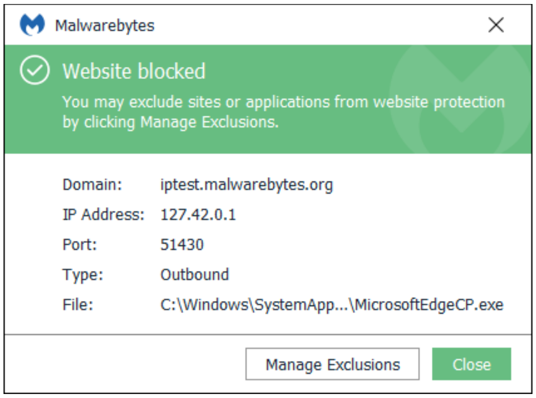


Potential threat automatically quarantined

Malwarebytes detected and automatically quarantined Potentially Unwanted Program (PUP). It is no longer a potential threat to your computer.

Type: Potentially Unwanted Program (PUP)
Name: PUP.Optional.DotPitch
Path: C:\Users\jbanning\Desktop\Test_PUP.exe

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.



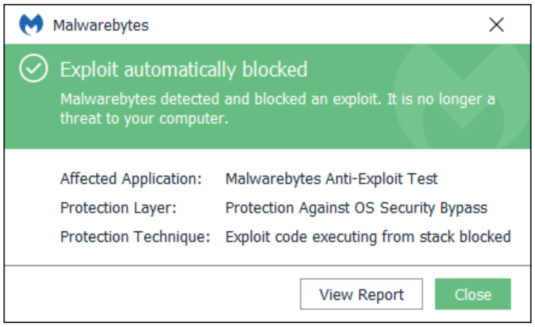
Website blocked

You may exclude sites or applications from website protection by clicking Manage Exclusions.

Domain: iptest.malwarebytes.org
IP Address: 127.42.0.1
Port: 51430
Type: Outbound
File: C:\Windows\SystemApp...\MicrosoftEdgeCP.exe

An attempt has been made by software present on your computer to contact a website suspected to be malicious, and has been blocked. This detection occurred as a function of real-time protection. You may allow access by clicking the Manage Exclusions link, which will redirect you to the Exclusions screens.

Please note: Unblocking a website out of convenience may result in damage being caused to your computer.

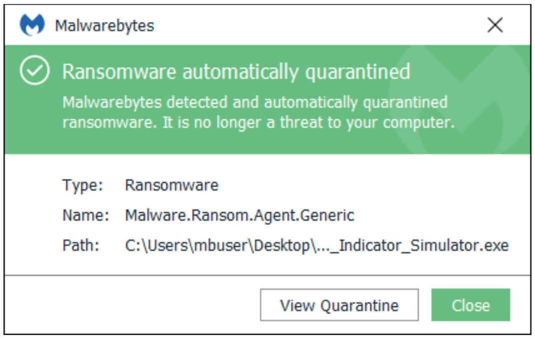


Exploit automatically blocked

Malwarebytes detected and blocked an exploit. It is no longer a threat to your computer.

Affected Application: Malwarebytes Anti-Exploit Test
Protection Layer: Protection Against OS Security Bypass
Protection Technique: Exploit code executing from stack blocked

Anti-exploit protection has prevented an attacker from exploiting your computer through a vulnerability.



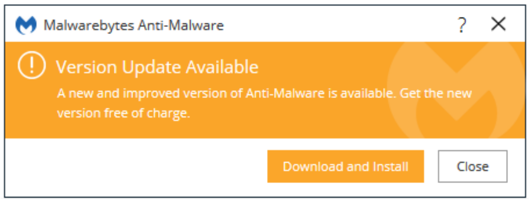
Ransomware automatically quarantined

Malwarebytes detected and automatically quarantined ransomware. It is no longer a threat to your computer.

Type: Ransomware
Name: Malware.Ransom.Agent.Generic
Path: C:\Users\mbuser\Desktop\..._Indicator_Simulator.exe

Anti-ransomware protection has prevented an attacker from exploiting your computer with suspected ransomware. The threat has been neutralized and moved to Quarantine.

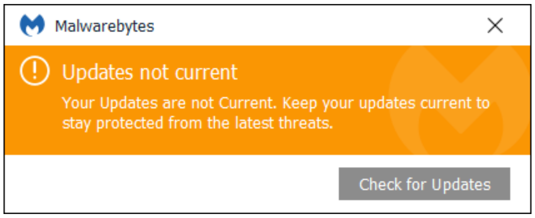
Update Notifications



Version Update Available

A new and improved version of Anti-Malware is available. Get the new version free of charge.

A program update for *Malwarebytes 3* is available. Click the Download and Install to get the latest program protection.

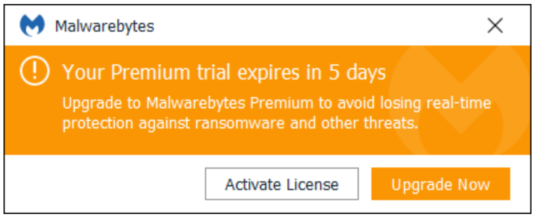


Updates not current

Your Updates are not Current. Keep your updates current to stay protected from the latest threats.

Your *Malwarebytes 3* updates are out of date. You may click the Check for Updates button to cause an immediate update. Failure to update will cause subsequent scans to use outdated protection rules, which could jeopardize the safety of your computer.

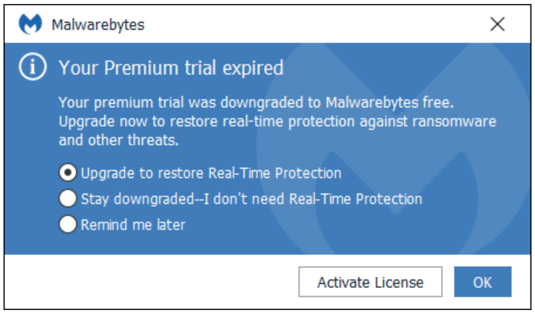
Trial/Subscription Notifications



Your Premium trial expires in 5 days

Upgrade to Malwarebytes Premium to avoid losing real-time protection against ransomware and other threats.

The Premium Trial is expiring in 5 days. You may choose to end the Premium Trial, purchase the annual subscription (which provides full access to all product features), or wait until the Premium Trial 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 bottom to do so now. **Please note** that if you end your Premium Trial early, you forfeit the time remaining on the Trial.

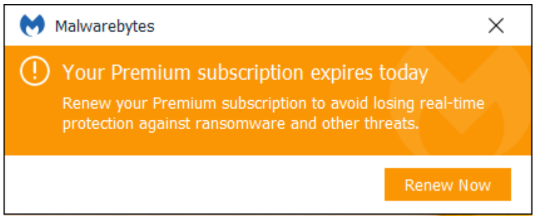


Your Premium trial expired

Your premium trial was downgraded to Malwarebytes free. Upgrade now to restore real-time protection against ransomware and other threats.

● Upgrade to restore Real-Time Protection
○ Stay downgraded--I don't need Real-Time Protection
○ Remind me later

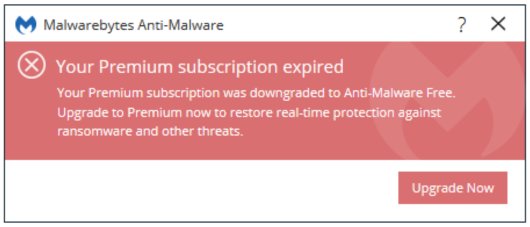
The Premium Trial has expired. Premium features have been disabled, including real-time protection, the ability to schedule scans, and automatic updates of the protection database. You may still execute scans on demand, as well as update the protection database. Click Activate License to enter a license which you have purchased, or click OK to acknowledge you are reverting to the free version.



Your Premium subscription expires today

Renew your Premium subscription to avoid losing real-time protection against ransomware and other threats.

If you do not have auto-renewal set up on your Malwarebytes account, you will begin to see this message thirty (30) days before the expiration of your subscription, counting down the number of days remaining on your subscription. You may click the **Renew Now** button to renew your subscription in a new browser window/tab.



Your Premium subscription expired

Your Premium subscription was downgraded to Anti-Malware Free. Upgrade to Premium now to restore real-time protection against ransomware and other threats.

If you do not have auto-renewal set up on your account and have not responded to pending expiration, you will see this notification a maximum of three times after your subscription has expired. At this point, you have reverted to the free version of *Malwarebytes 3*. Premium features have been disabled. You may click the Upgrade Now button to renew your subscription in a new browser window/tab.