Malwarebytes for Windows User Guide

Version 3.5.1

8 May 2018

Notices

Third Party Project Usage

Malwarebytes software is made possible thanks in part to many open source and third party projects. A requirement of many of these projects is that credit is given where credit is due. 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.

Table of Contents

Table of Contents (continued)

Introduction

Malwarebytes for Windows ("Malwarebytes") 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*, 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 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 to behaviorally detect ransomware.
5. Revamped Anti-Malware and Web Blocking engines, offering more aggressive detection techniques.
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* User Guide!

What's New in Malwarebytes for Windows

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

Performance/protective capability

- Added support for Hypervisor Code Integrity (HVCI) and Device Guard to meet Microsoft compliance requirements
- Improved the remediation process so fewer reboots are required
- Improved the accuracy of the Web Protection module
- Improved driver management for increased stability
- Continued improvements to overall protection, detection and remediation

Usability

- Updated the dashboard design to better showcase Malwarebytes real-time protection features
- Updated Notification Center behavior to make it easier to dismiss
- Numerous other user interface and copy enhancements

Stability/issues fixed

- Fixed issue where anti-ransomware module could cause high CPU and memory use
- Fixed an issue where Malwarebytes would open to the scan tab instead of the dashboard
- Fixed reported crashes related to Web Protection
- Fixed several translation issues
- Addressed other miscellaneous defects

System Requirements

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

- **Operating System:** Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista† (Service Pack 1 or later), Windows XP† (Service Pack 3 or later, 32-bit only)

  PLEASE NOTE: Anti-ransomware protection is not supported for Windows XP or Windows Vista, due to architectural constraints.

- **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**

---

† *Malwarebytes for Windows* Version 3.5.1 or below required. You can read more on our website:

https://links.malwarebytes.com/docs/mb3_legacy

WARNING: If you are upgrading from *Malwarebytes Anti-Malware* version 2.x and have enabled Malwarebytes' self-protection feature, please disable it prior to initiating the upgrade. It prevents the *Malwarebytes* installation program from doing its job.

Installation

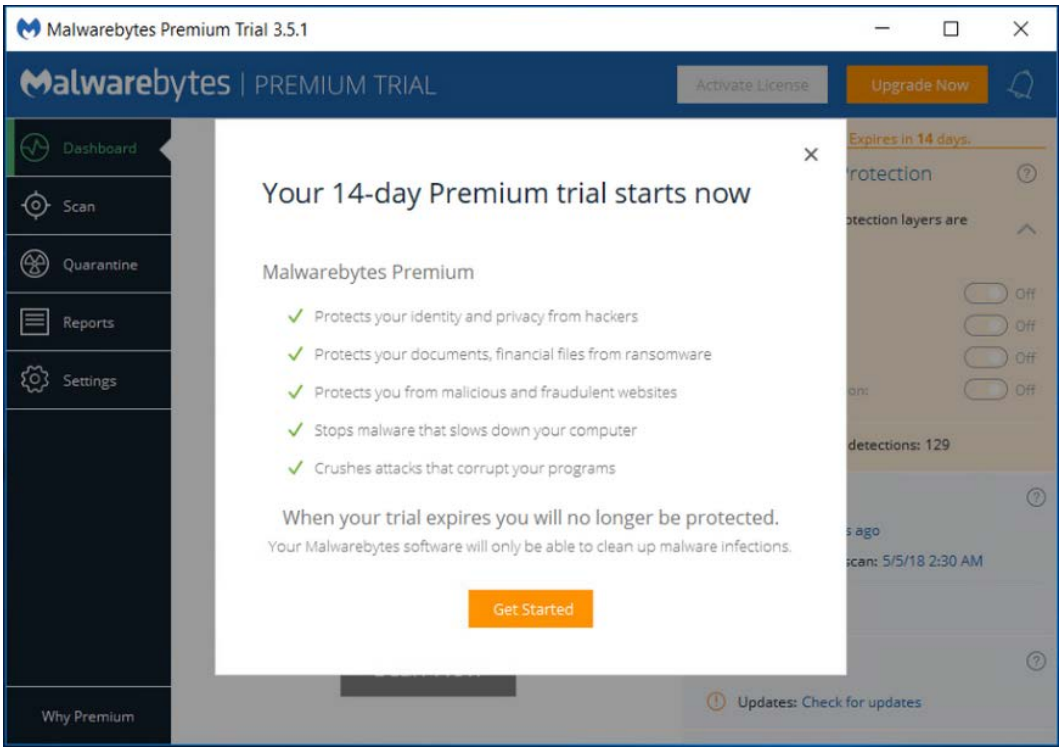
To begin the installation, double-click on the *Malwarebytes* installation file which you downloaded. If you are installing *Malwarebytes* on a Windows version newer than Windows XP, a Windows dialog box will be presented in the middle of your screen, labeled **User Account Control**. Verify that the publisher is listed as Malwarebytes Corporation and click **Yes**. This Windows security feature assures limited application capabilities unless and until you authorize higher capabilities. Installation will begin once this has been approved. The installation program guides you and allows you to provide alternate information if you do not wish to accept defaults. Each screen also allows you to terminate installation if you do not wish to continue.

Free, Premium Trial or Premium?

Before you begin, we want to let you know that throughout this guide, you will see references to the Free, Premium Trial, and Premium versions of *Malwarebytes*. 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*.

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

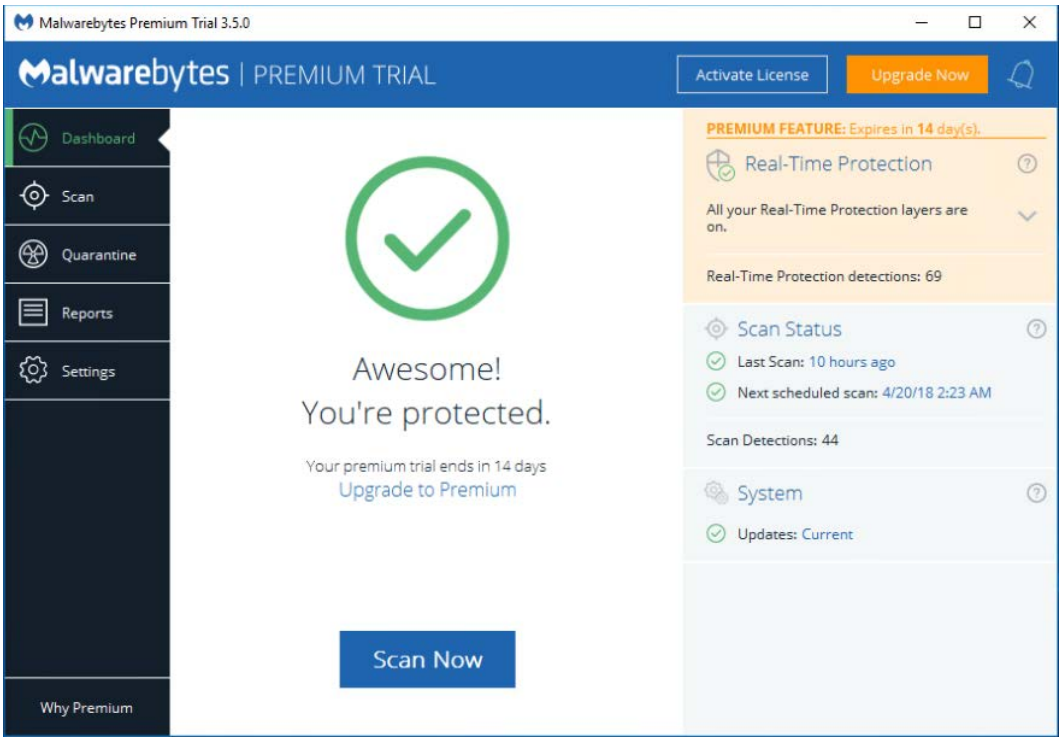
These benefits are also shown in the *Malwarebytes* interface immediately after it has been installed. See below….



The Premium 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 Premium Trial is available at no cost, but you can only use it one time for each version of *Malwarebytes*. The Premium Trial is automatically started during installation. Once installed, the program provides options to convert from Free to Premium, and from Premium Trial to Premium.

If you elect to use the Premium 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.

If you are a new *Malwarebytes* user, or are a free/Premium Trial user upgrading to this version, you will be alerted that a scan has not been run. Click **Scan Now** and Malwarebytes will run a scan for you. After the scan (and cleanup, if needed) has been completed, you will see the user interface as shown below.

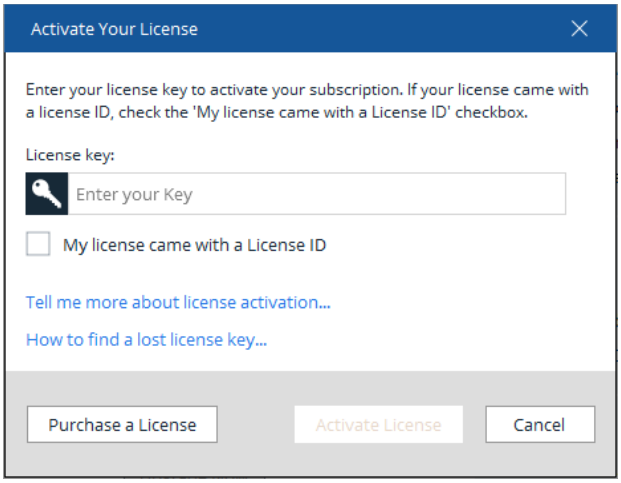


Please take note of the **Why Premium** button in the lower left corner. Click that button for a brief slide show that describes the differences between Free and Premium modes. While *Malwarebytes* does an effective job of disinfecting your computer after an attack, there is no replacement for preventing the attack from ever happening.

If you have already purchased a license, you may wish to activate your copy of *Malwarebytes* 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* user interface.

Activation

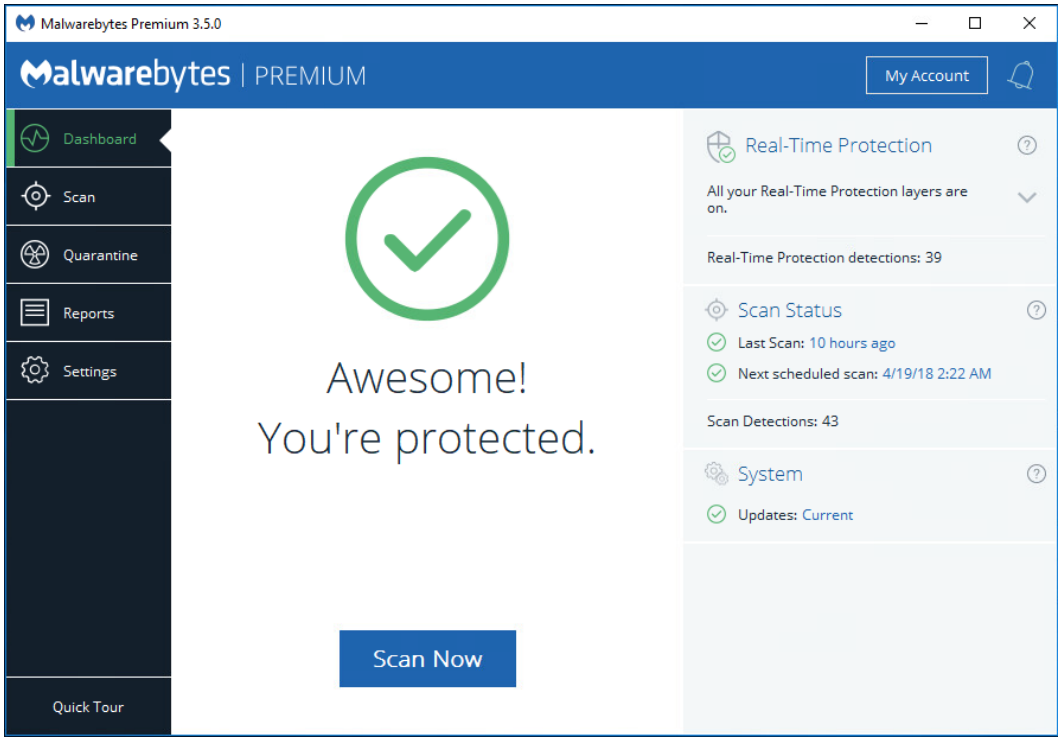
Malwarebytes is available for users of any modern Windows client to download and install at no cost. You can also purchase an annual subscription, which entitles you to take advantage of real-time protection, scan/update scheduling and access policies. If no license has been installed into the product, the blue title bar at the top of the screen will show two buttons, **Activate License** and **Upgrade Now**. When clicked, **Upgrade Now** launches a browser window which opens to the Malwarebytes web site pricing/purchase page. 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.



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* screen will refresh, as shown below.



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

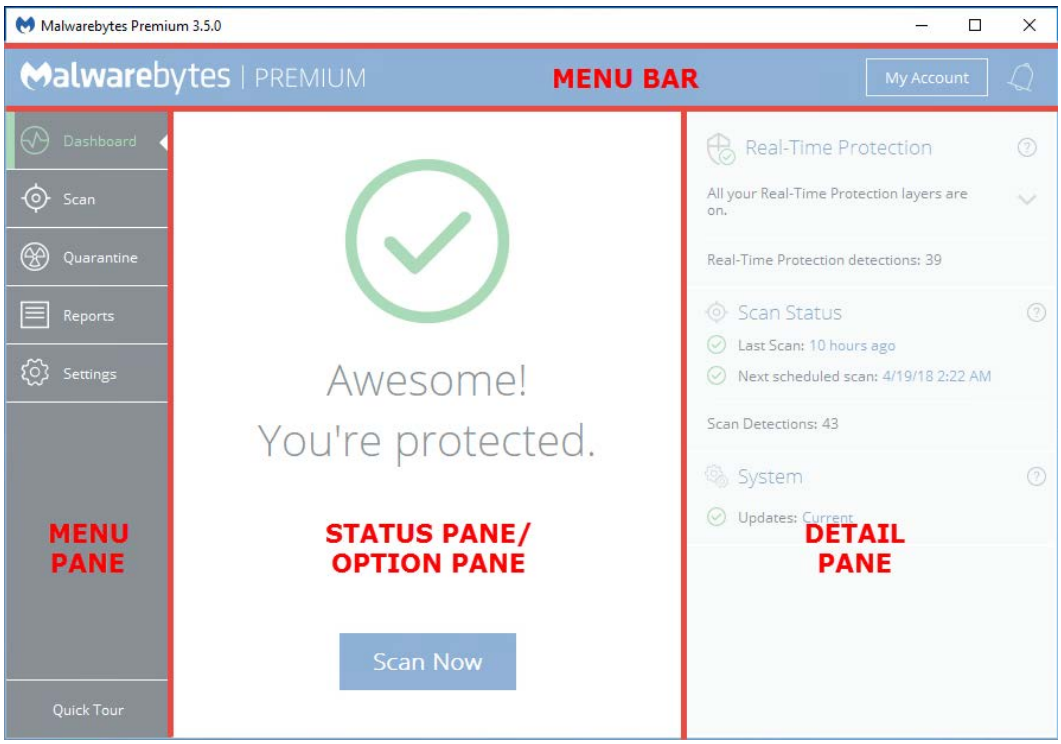
A Final Word about Administrative Rights

If you installed *Malwarebytes* from a downloaded installation file, you automatically started a Premium Trial, and were 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* 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* is launched for the first time.



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

Menu Bar

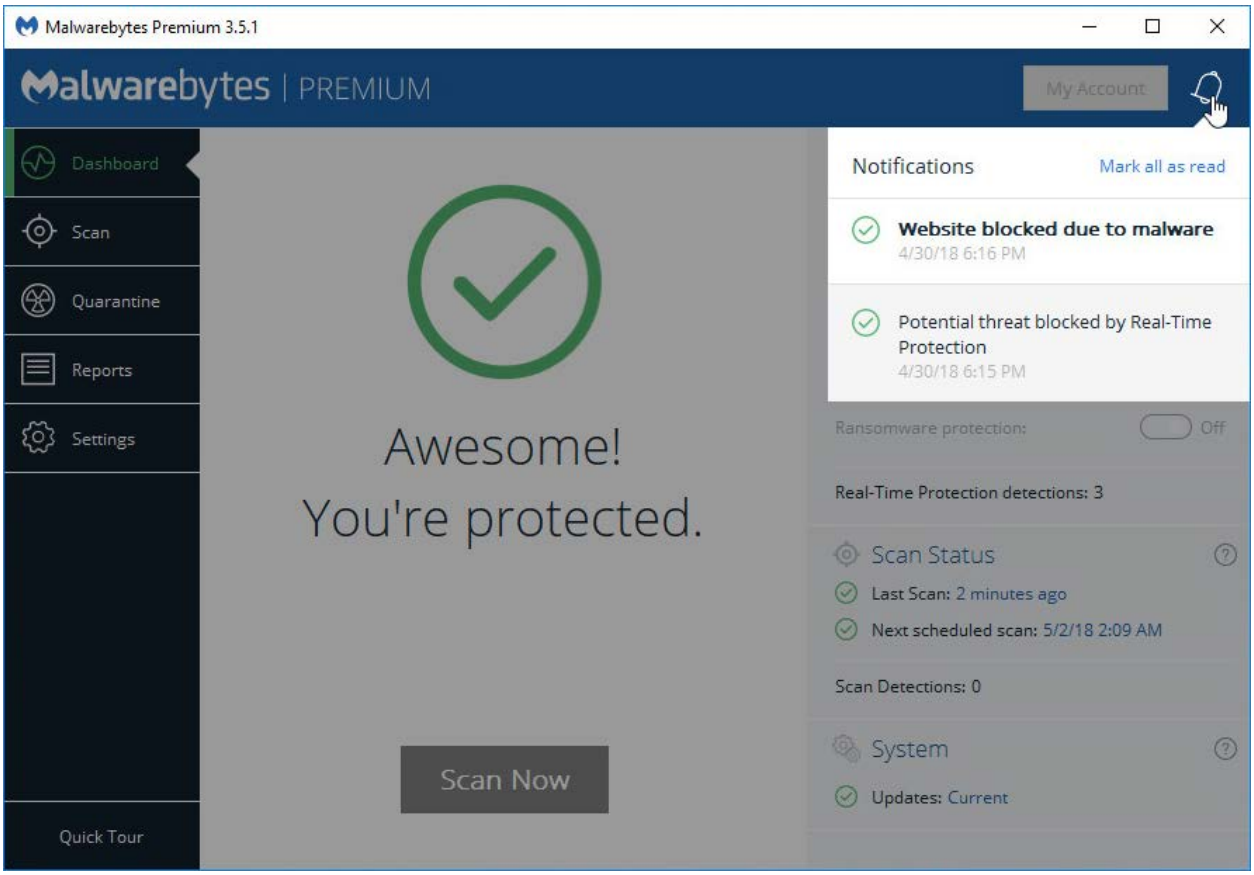
The Menu Bar is displayed at the top of the screen at all times. There are two buttons in the Menu Bar. A description for both follows.

My Account

This button will take you to the setting options to manage your *Malwarebytes* subscription(s) and license(s). For more information, please refer to pages 34-35 of this guide.

Notification Center

The Notification Center provides a convenient location to view recent notifications generated by *Malwarebytes*. Clicking the icon will show the 5 most recent notifications. You may scroll down to view up to 25 notifications by using your mouse wheel. You can view additional details for each notification by clicking it – *Malwarebytes* will bring you to the relevant screen. The Notification Center will not appear until *Malwarebytes* generates a notification. If you do not see the icon, you have not yet received any notifications.



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, detected threats, and threats which have been removed.
- **Settings:** Configure every aspect of *Malwarebytes*, 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.

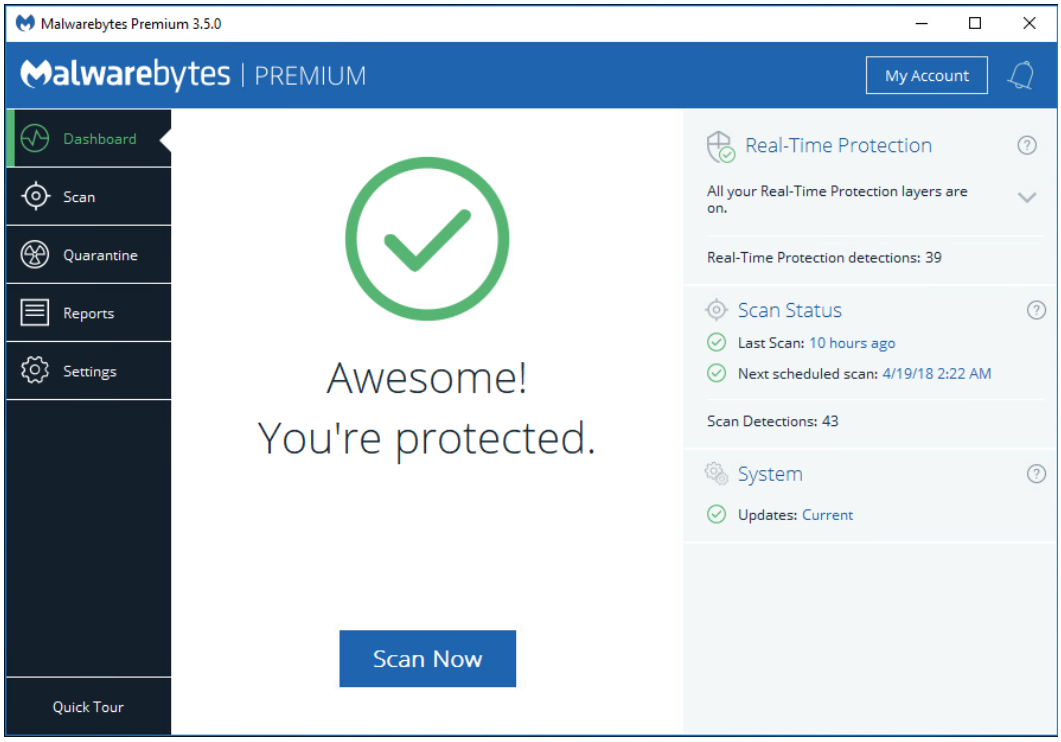
When any menu option other than the Dashboard is selected, all space except the space used by the Menu Pane is allocated to the selected menu option. This provides sufficient room for information pertaining to any menu option to be cleanly displayed.

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* is launched, the first page visible to the user is the *Dashboard*. It provides program status, and acts as a *launch pad* for all program operations. A screenshot of the user interface – featuring the Dashboard – is shown below for reference.



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. (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 3-7 days)
  - Renew to avoid losing protection against malware, bad websites, and other threats
- **Color: red (critical problem)**
  - Your Premium Trial ends in <x> days. (trial expiring in 0-3 days)
  - Your trial has expired
  - Renew to avoid losing protection against malware, bad websites, and other threats
  - 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. By default, the application will show a condensed view of this information. You can expand this section by clicking the arrow icon on the right side of the screen. This expanded view will allow you to quickly enable or disable individual Protection layers. More information on each layer is available on page 28 of this guide. **Please note** that real-time protection is enabled only for *Malwarebytes Premium* and *Malwarebytes Premium Trial* users. This feature is not available if you are using the Free version. You can click the question mark icon to view the *Malwarebytes User Guide* on the Malwarebytes website. This behavior is consistent throughout the program. This panel also shows the total number of threats detected by real-time protection.

Scan Status

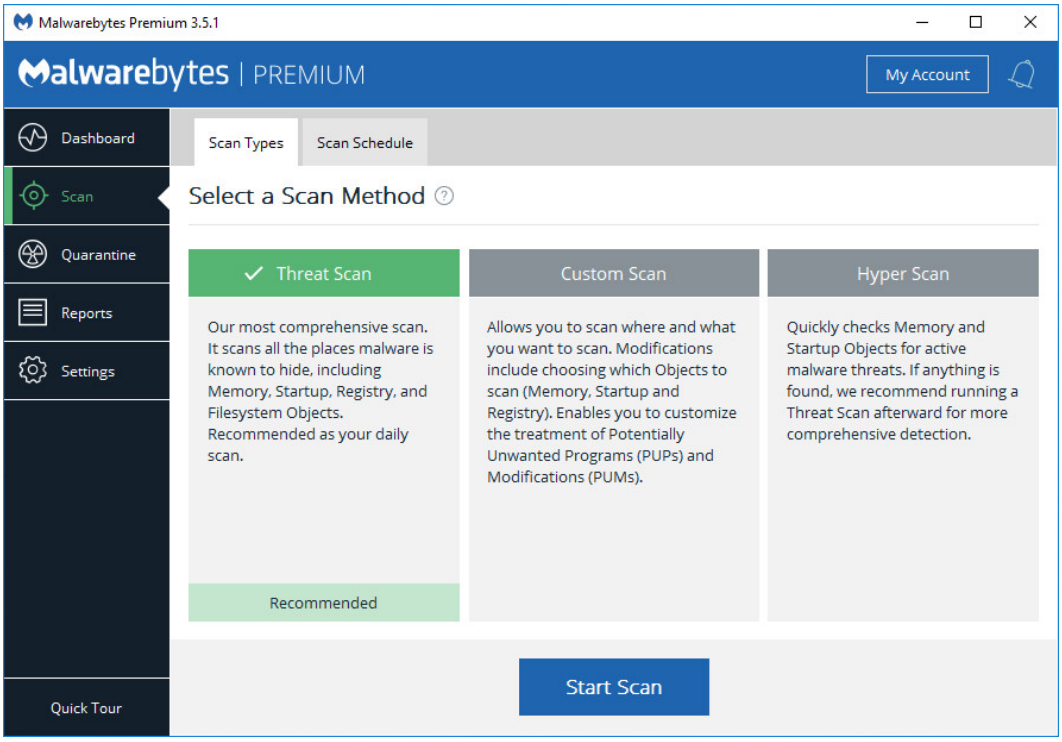
This panel shows your scanning activity at a glance. You can easily see when the last scan was completed, when the next scan is scheduled, and the total number of threats that have been detected during scans.

System

This panel shows the status of your protection updates.

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.



On this screen, you may select the Scan Method and the Scan Schedule. Let's look first at Scan Methods. 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 Premium Trial modes. Please note that global scan settings used by Threat Scans and Hyper Scans are selected in Settings (see pages 30-31). Following are more detailed descriptions of each of the scan modes.

Threat Scan

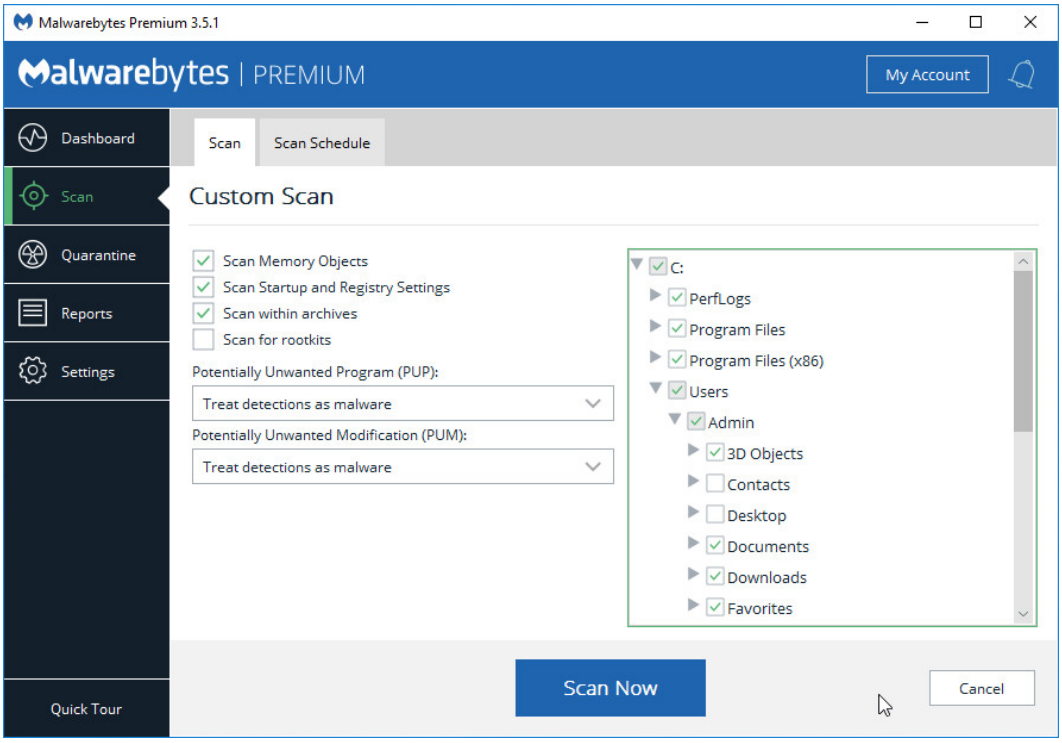
This method of scanning detects a large majority of threats that your computer may be faced with. Areas and methods tested include:

- **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 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 two 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

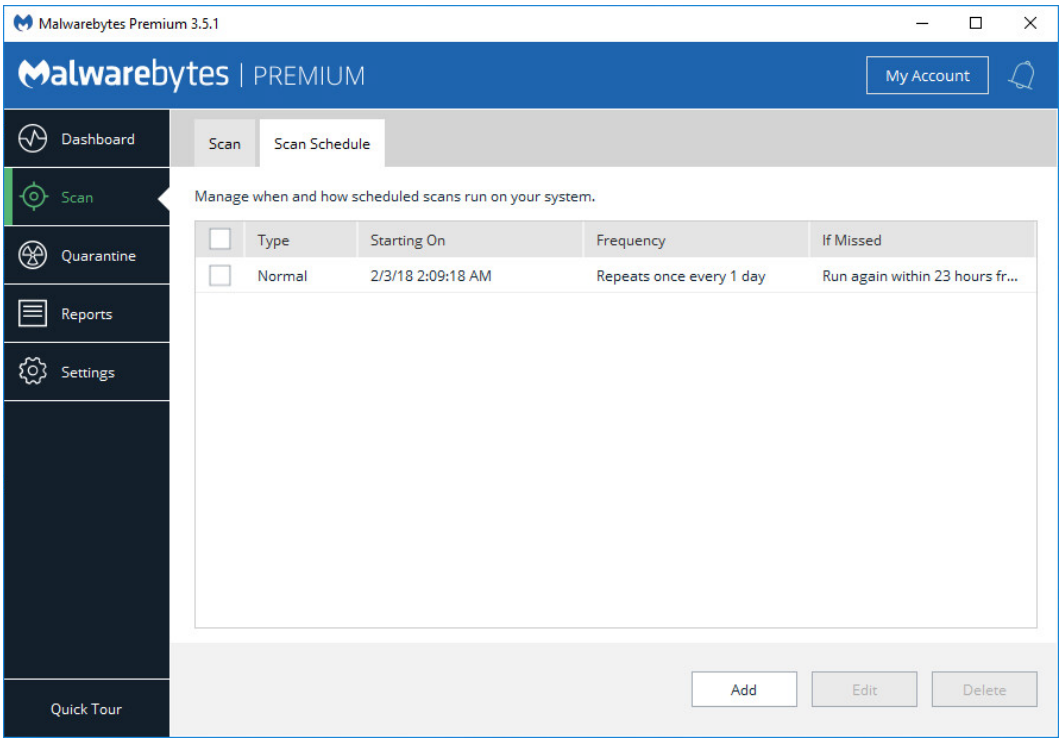
This scanning option is only available to users of *Malwarebytes Premium* and *Malwarebytes Premium Trial* versions. This method of scanning is limited to detection of immediate threats. Areas and methods tested include:

- **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.

Scan Schedule

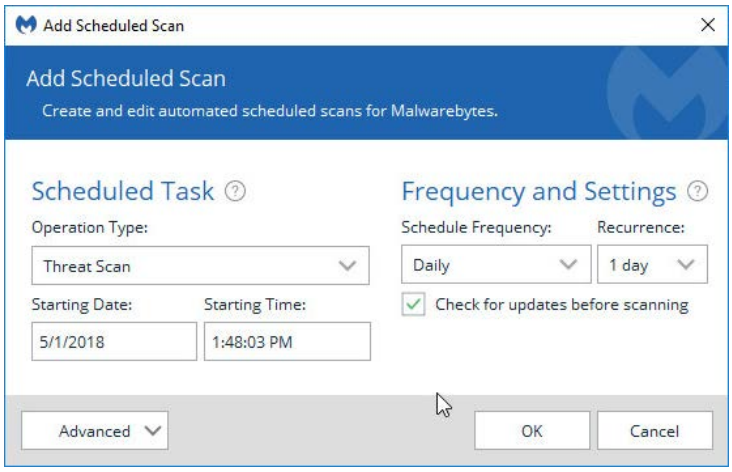
This tab allows users of the Premium and Premium Trial versions to add, edit and remove scheduled scans to be executed by *Malwarebytes*. This feature is not available to users of the Free version. A screenshot of this tab is shown below.



One scheduled scan is defined when *Malwarebytes* is installed. Premium and Premium Trial users are free to modify or delete scans at will, while Free users are provided with a single monthly scheduled scan. **Please note** that if the initial task is deleted without a replacement task being defined, your *Malwarebytes* 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 Add Schedule screen is shown here.



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

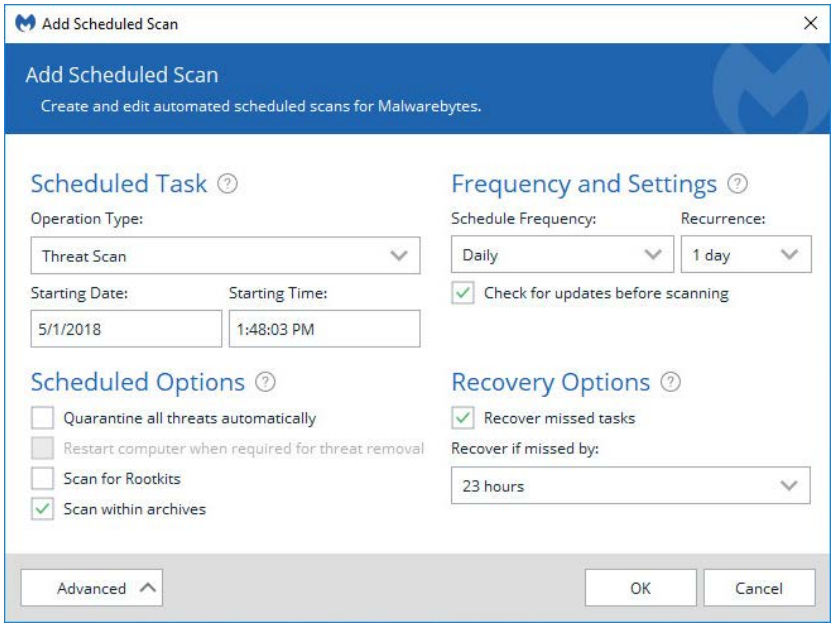
- Threat Scan
- Custom Scan
- Hyper Scan

Scan types have been previously discussed in the Scan section of this guide (pages 11-19). 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.



In Advanced Mode, we add options which tailor the scan 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.

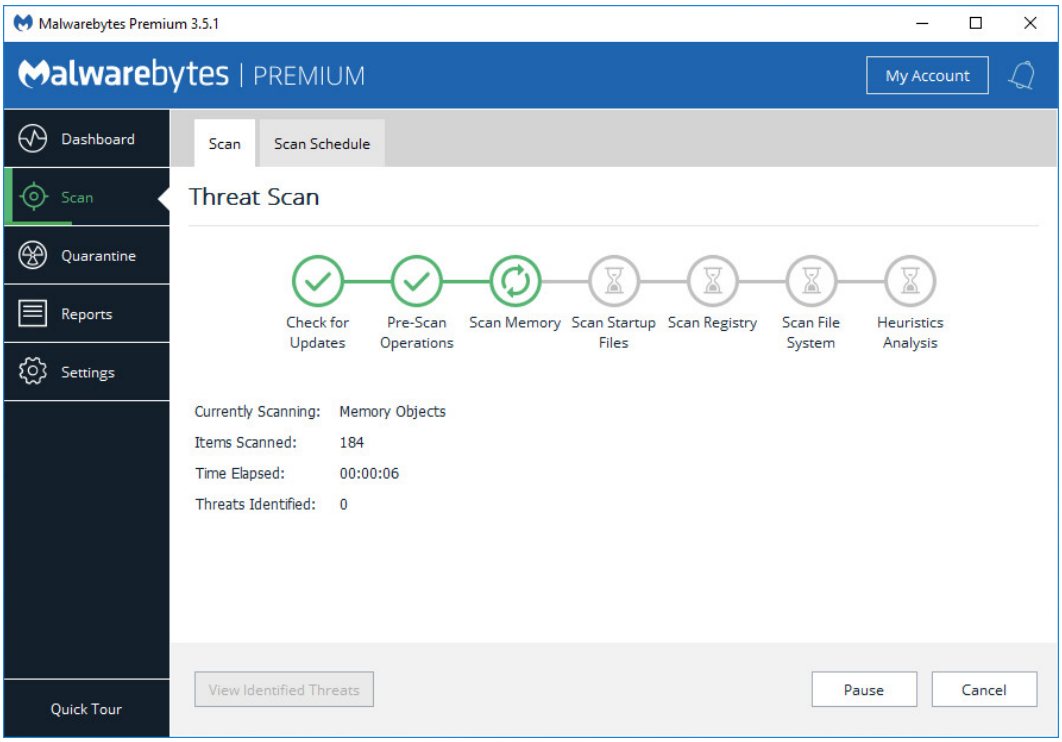
- **Quarantine all threats automatically:** This option determines if a newly-detected threat would be automatically quarantined, or if you would be notified so that you could choose a course of action. While automatic quarantine may seem to be the best course of action, it could have negative implications 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 two levels deep within archive files. If 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.

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.

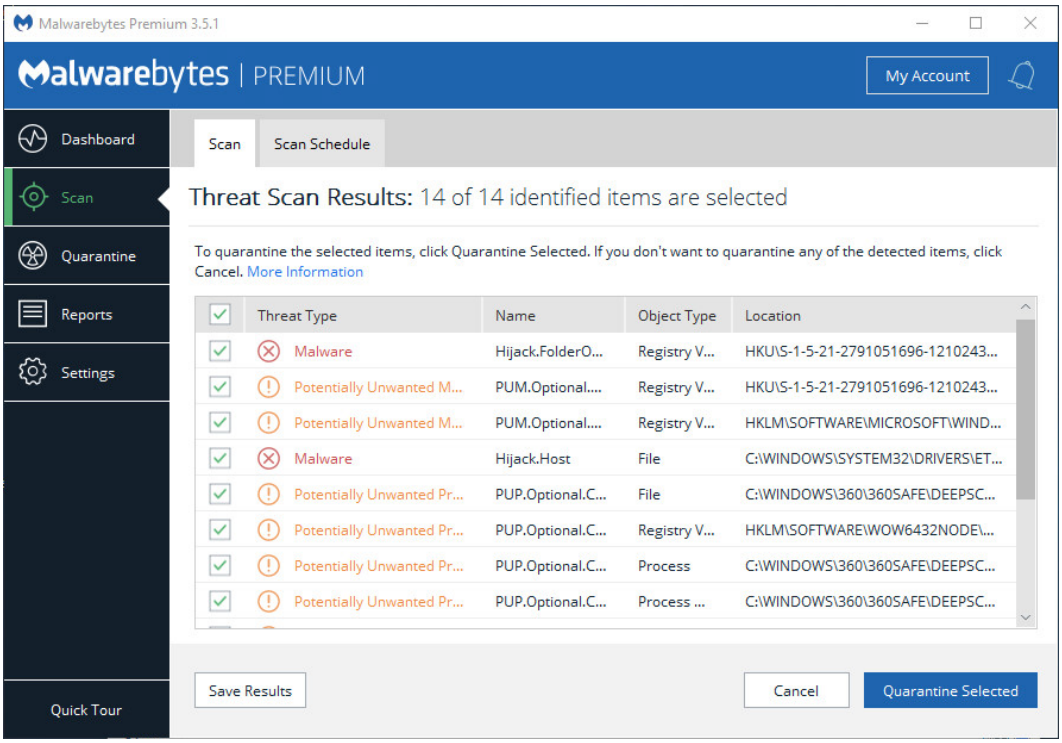


The progress bar shows milestones for each phase of the scan, with each milestone represented by a green or gray symbol. In this screenshot, some milestones are shown with green checkmarks, indicating that phase of the scan has been completed. *Scan Memory* is represented by an animation which indicates that this phase of the scan is currently being performed. The remainder of the tasks are shown as grey hourglasses, and are yet to be started.

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, fourteen threats were detected.

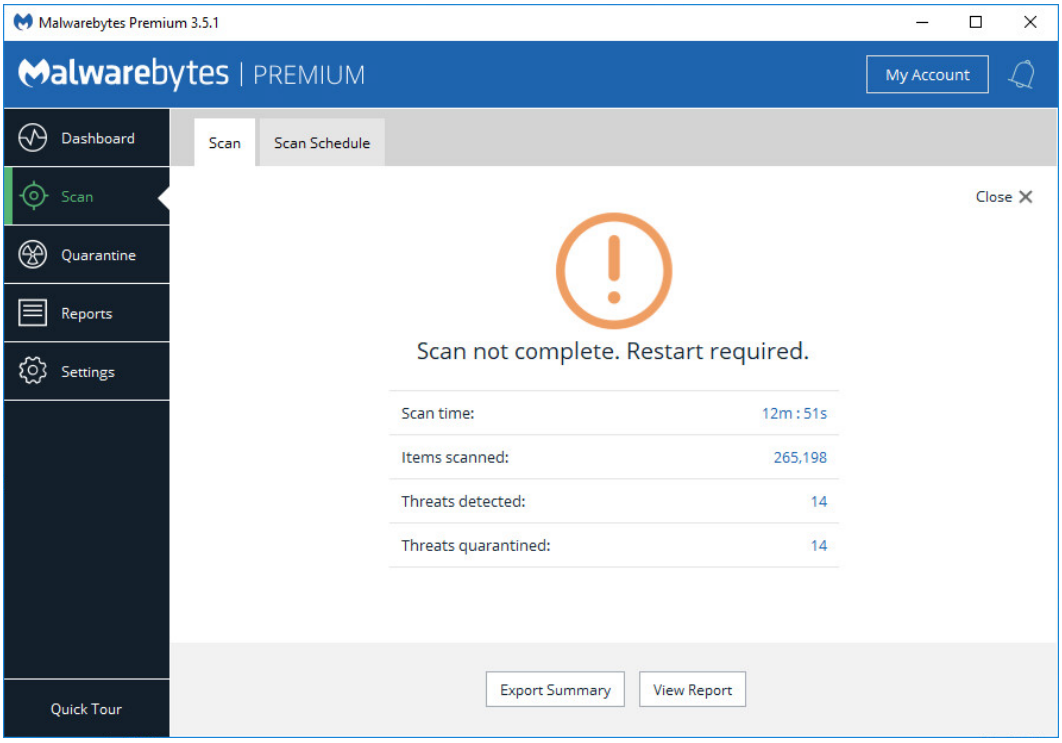


You may move threats to Quarantine by selecting the threat (using checkboxes to the left of the threat's name) and clicking **Quarantine Selected**. If any threats are not selected to be moved to Quarantine, you will be prompted to Ignore Once, Ignore Always, or Cancel. Ignore Once will result in the 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.

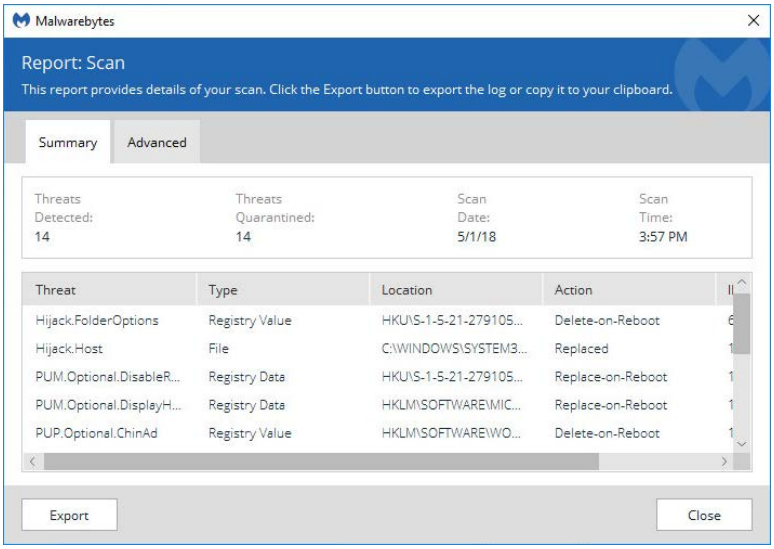
Threats which have been moved into Quarantine cannot harm your computer. They are neutralized as part of the Quarantine process. Please see *Quarantine* (page 20) for further information.

Scan Summary

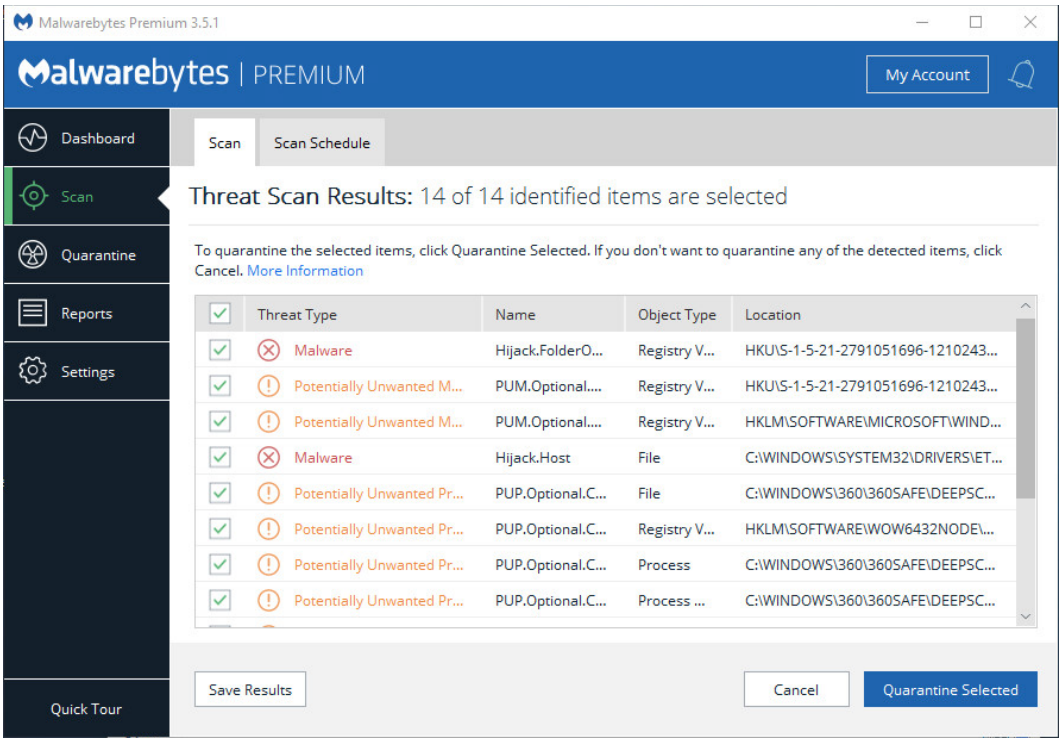
The final screen to be displayed as part of a scan is the Scan Summary. It provides summary information about the scan, and allows you to view scan detail on screen, or export scan summary or scan detail to a text file. A screenshot of the Scan Summary is shown below. Free and Premium Trial users will see a reminder of the value of a Malwarebytes subscription on this page as well.



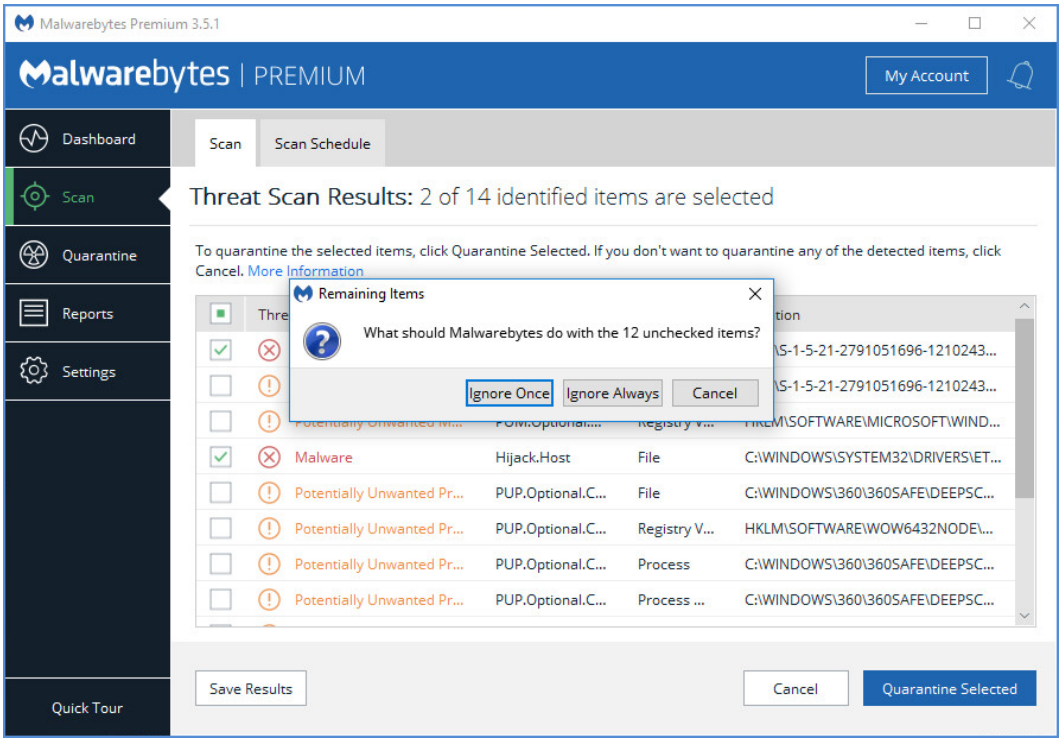
Clicking the View Report button displays the Scan Report for the scan just completed. It is shown here as well.



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, fourteen 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, as is the number of threats selected for removal.

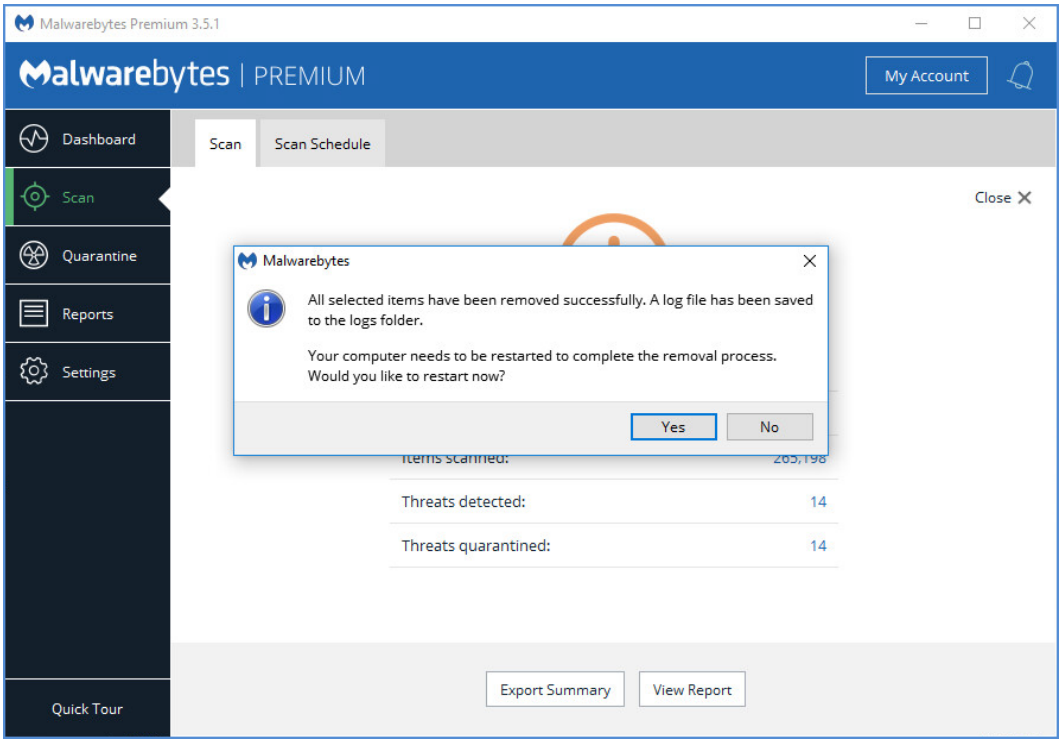


In order to demonstrate the behavior of this screen, we will uncheck some of the threats. This indicates that only the checked threats are to be removed. Clicking the Quarantine Selected button results in the screen shown below.



Threats that were not selected still require 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 a 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

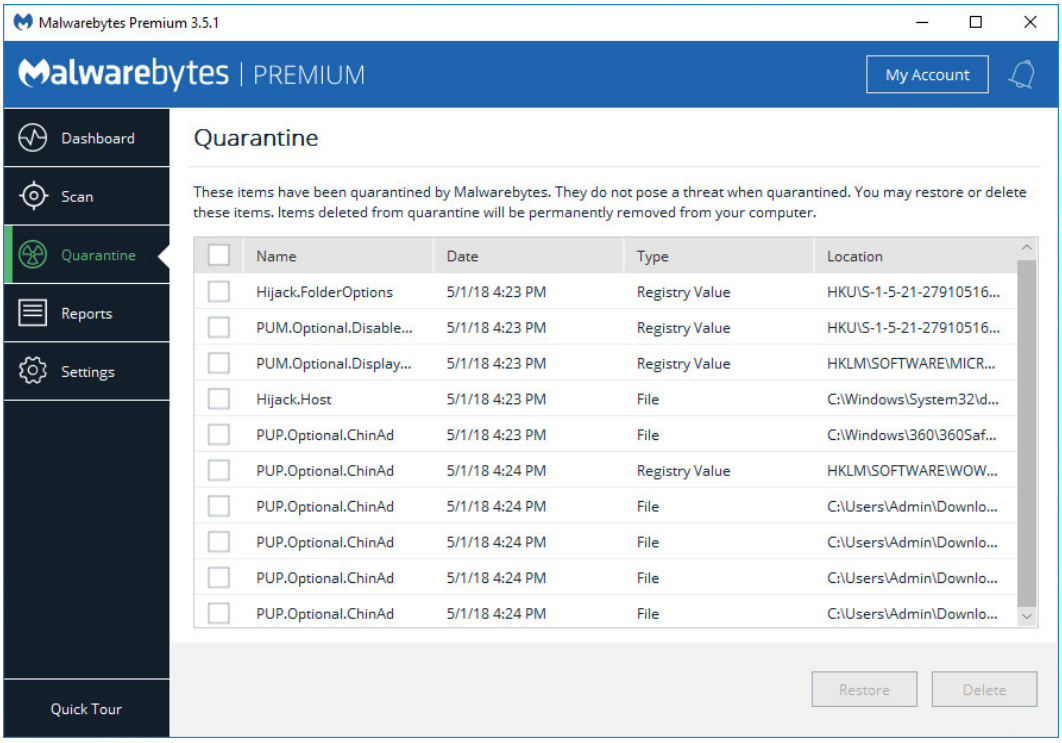
scanned in the future. Clicking Cancel keeps you on this screen until you choose how to handle all detected threats. Once a disposition has been selected for all detected threats, the screen below will be displayed.



Although threats have 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.

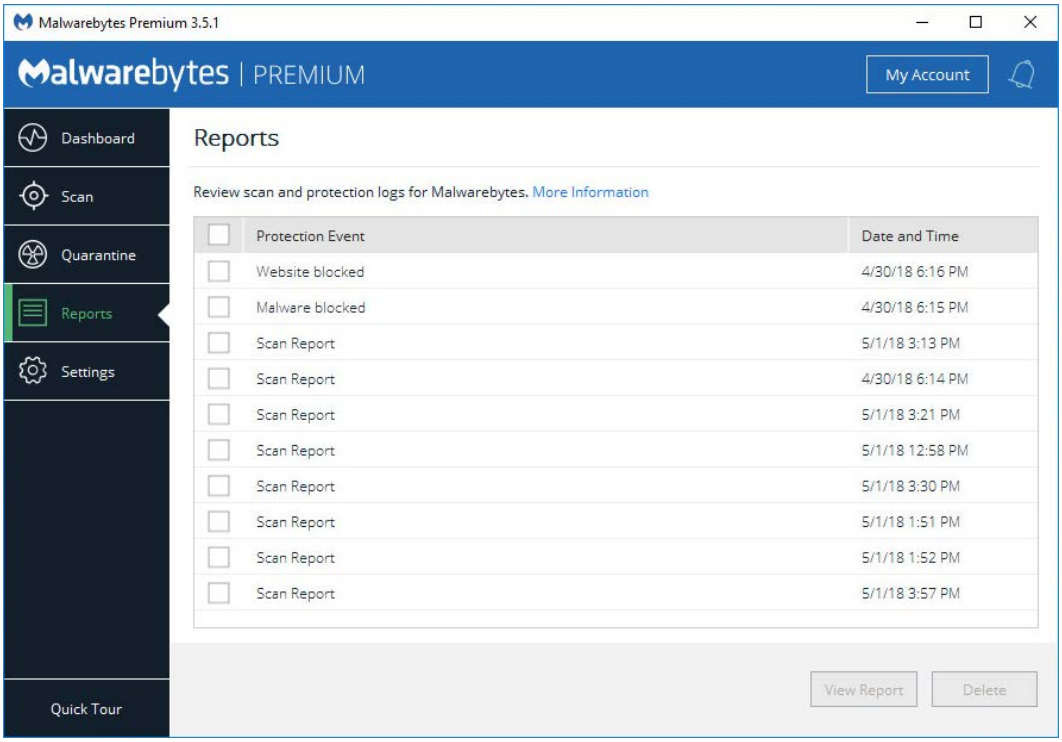


Quarantined items are shown in a table format, with pertinent information presented to help you determine what action needs to be taken. Each item listed has a checkbox in the leftmost column. Check the checkbox to restore or delete the item. Please note that the Restore and Delete buttons are greyed 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.

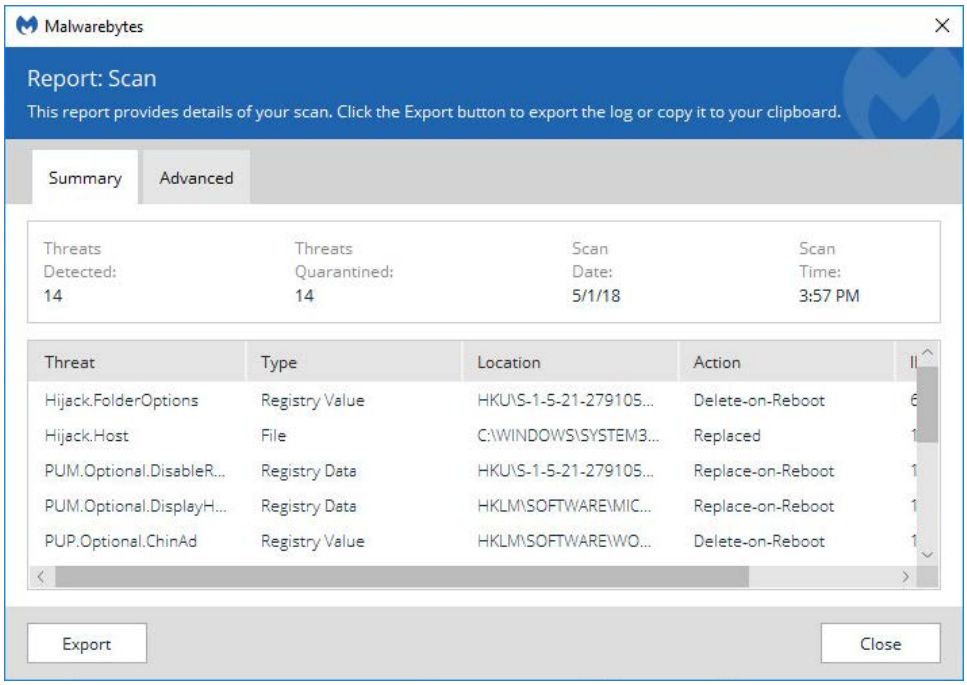
Reports

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.

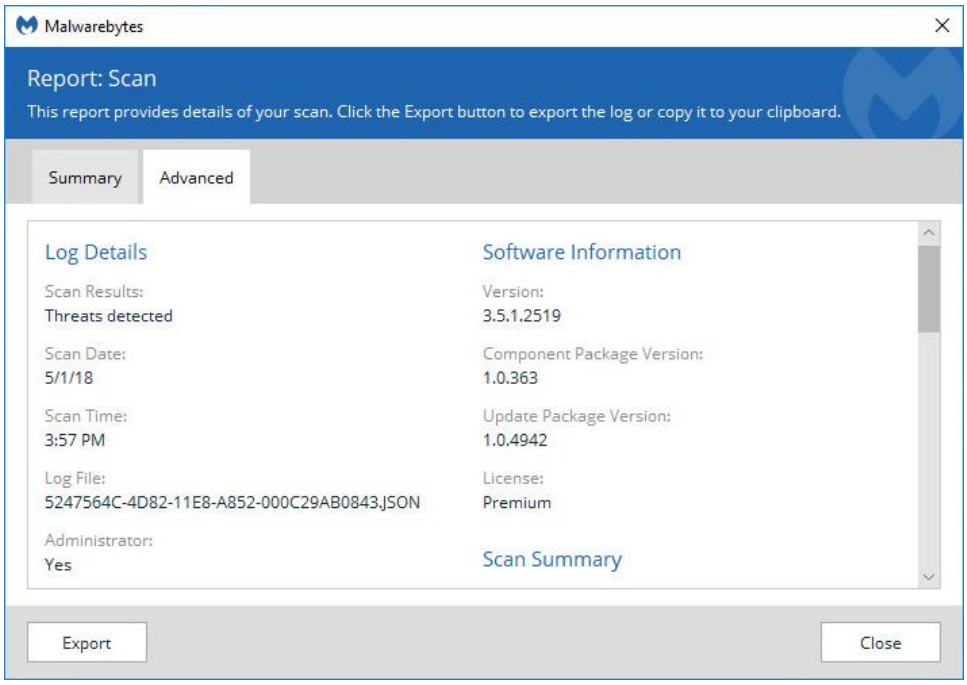


Selected reports may be viewed on screen, or exported to a text file for later viewing. Opening a report will display a summary of the event. You can click the Advanced tab to view more information about the event. Details displayed for *Protection Events* will be relevant to the type of event shown. Please note that only manual (on demand) scans are available for users of the free version of *Malwarebytes*.

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



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 contains a summary of the scan. You can click the Advanced button to view more details, as shown here:



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 *Malwarebytes* operational settings. We have grouped settings by the areas/functions which they control into tabs 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.

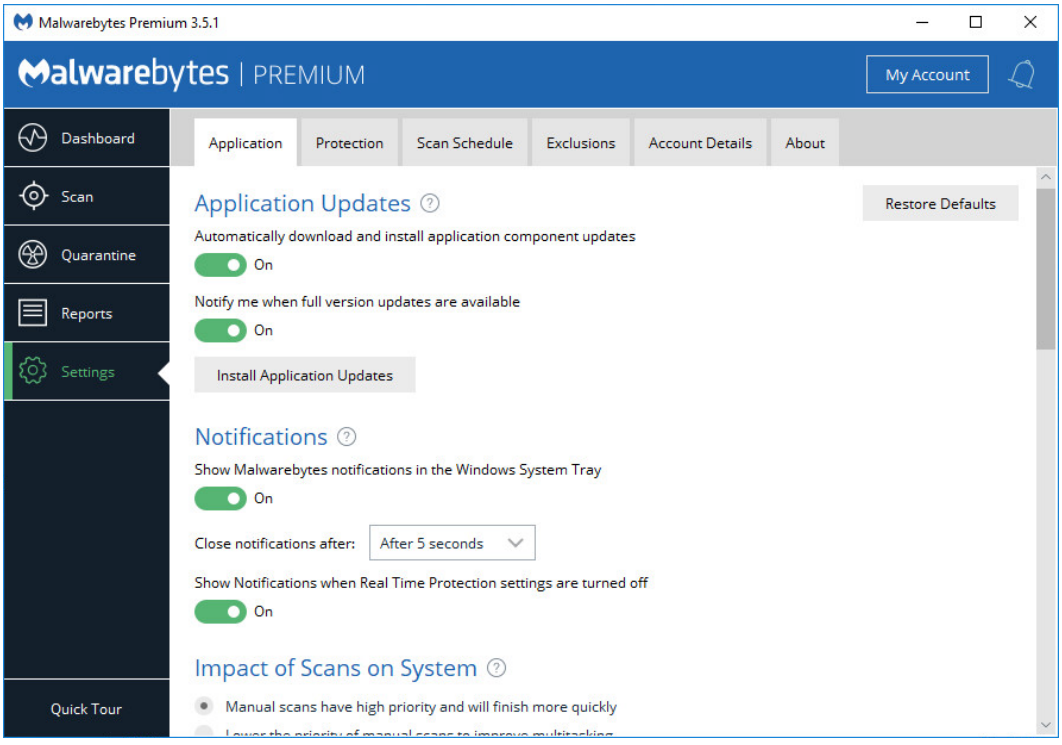
- **Application Settings:** Settings that affect *Malwarebytes*, as well as how it coexists with Windows.
- **Protection Settings:** How *Malwarebytes* should protect you during scans and (for Premium/Trial mode users only) Real-Time Protection.
- **Scan Schedule:** When *Malwarebytes* should execute 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* as a whole, and for various components of the program which may be updated individually. Malwarebytes company 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* interacts with many aspects of your computer's operating system. A screenshot is shown below.



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 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* 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* 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 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

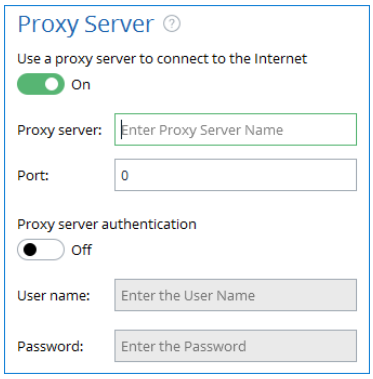
This setting determines the language used throughout. This is pre-set, based on the language used during program installation. It can be modified at will.

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*, 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.

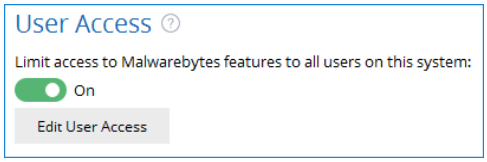


By default, *Malwarebytes* does not use a proxy. If configured to do so, the bottom panel will change to provide configuration options as shown in the screenshot shown here.

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.

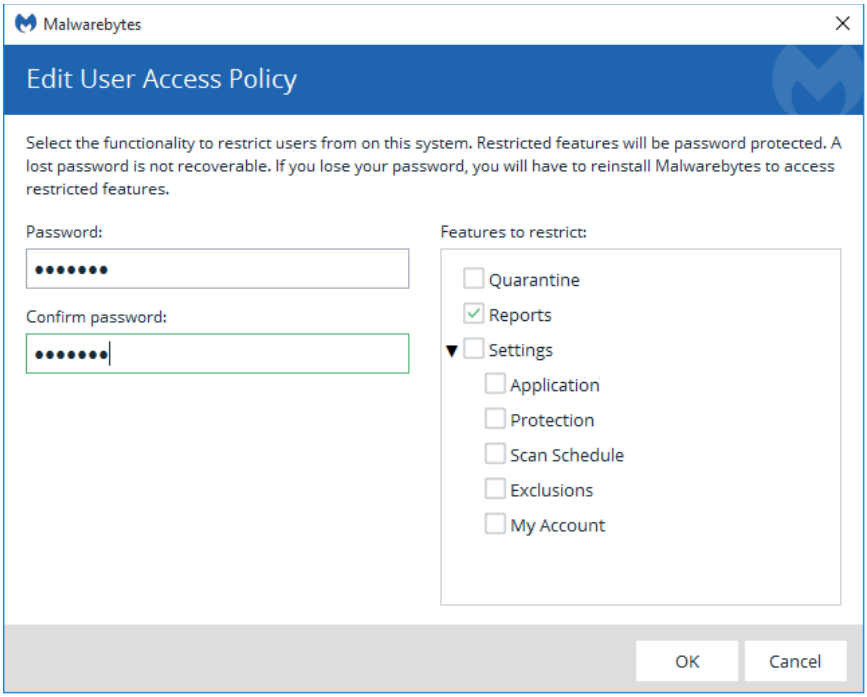
User Access

This slider allows users of *Malwarebytes* Premium and *Malwarebytes* Premium Trial versions to restrict access to various features and functions in *Malwarebytes* 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.

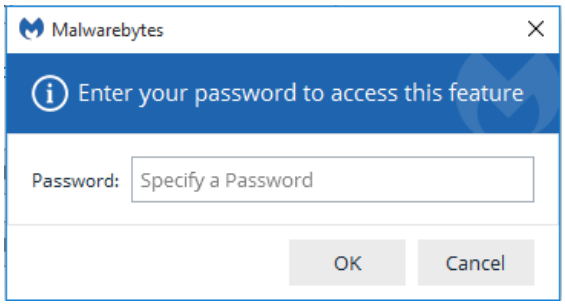


When the Edit User Access button is clicked, a new window opens directly above the *Malwarebytes* program screen to restrict access to selected areas of the program only to those users who possess the password. The password is also defined on this screen.

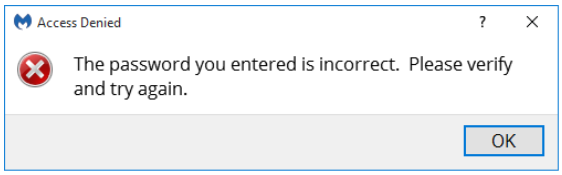
WARNING: This password is not recoverable. If you lose your password, you will have to reinstall *Malwarebytes* to access restricted features.



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.



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



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.

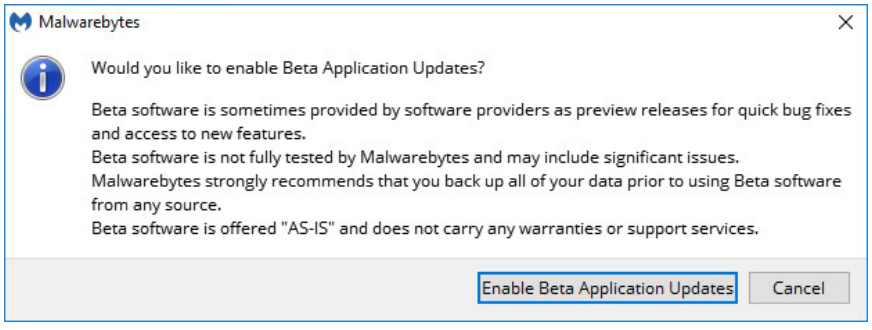
Windows Action Center

You may have noticed an icon in your system tray with a red X superimposed over a 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* or *Malwarebytes Premium Trial* 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* 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* program status will always appear in Action Center.
- **Never register Malwarebytes:** *Malwarebytes* program status will never appear in Action Center.

Beta Application Updates

Some Malwarebytes users want to try the newest features as soon as they are available, while some prefer to wait until the product is released. We have added this program setting so that if you want the latest and greatest immediately, we can deliver it to you automatically. When you enable this setting, you will see the following dialog box.



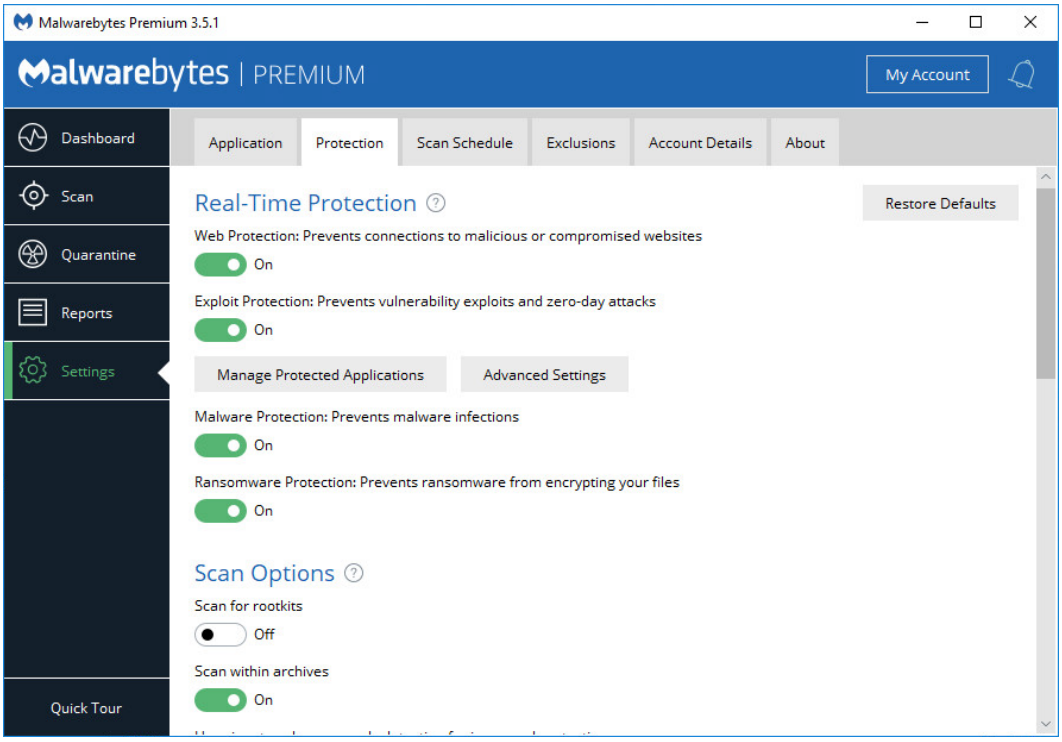
Usage and Threat Statistics

If you check this box, you will be sending us information to help us do our jobs. We like to know what countries *Malwarebytes* is being used in, and the breakdown of Premium, Premium Trial, and Free versions. Our Research organization likes to keep track of what malware we are detecting and how often. We learn that from what you send us, and helps 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* 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.

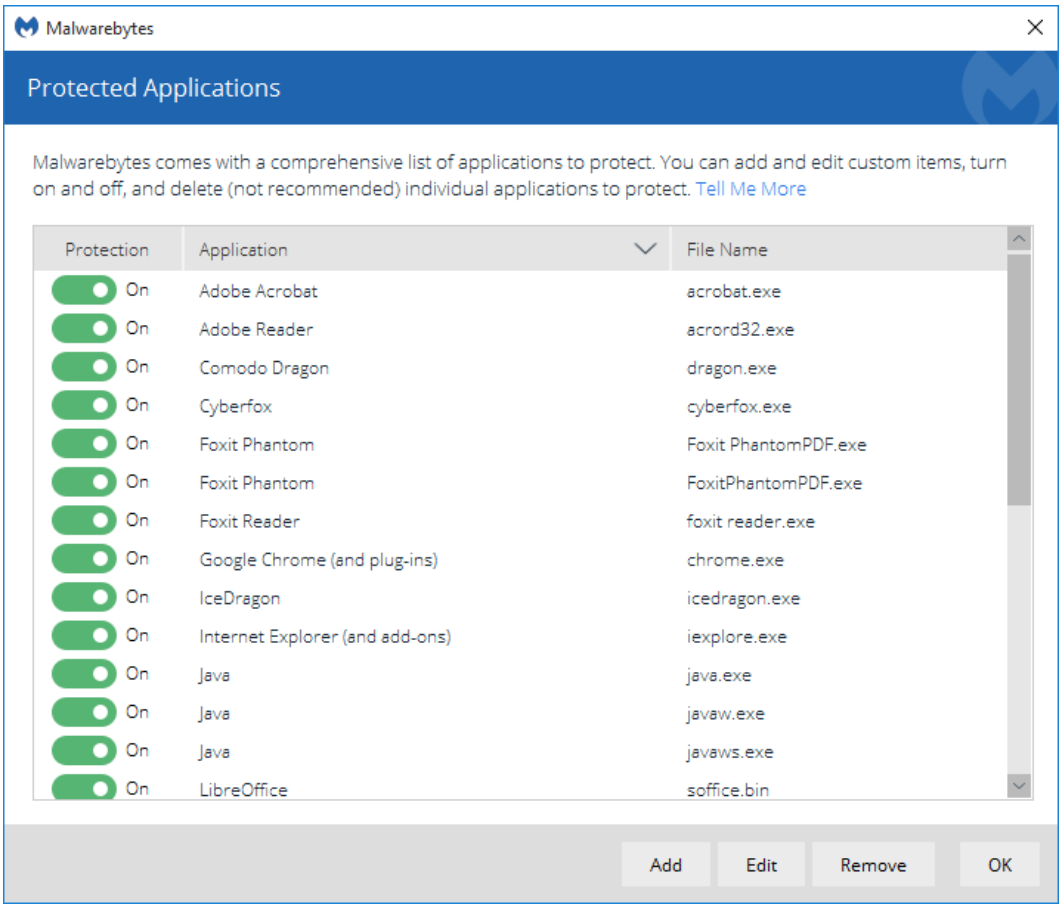


Real-Time Protection

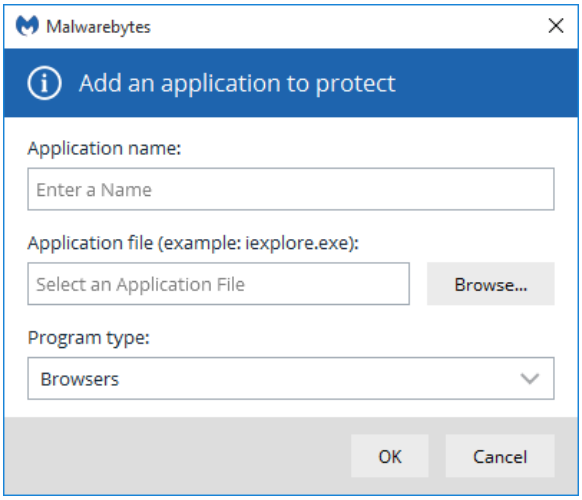
Malwarebytes offers four different types of real-time protection. These features are available only to users of the Premium and Premium Trial modes. It is important to note that Premium Trial users who do not convert to a Premium subscription will lose all real-time protection features at the end of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



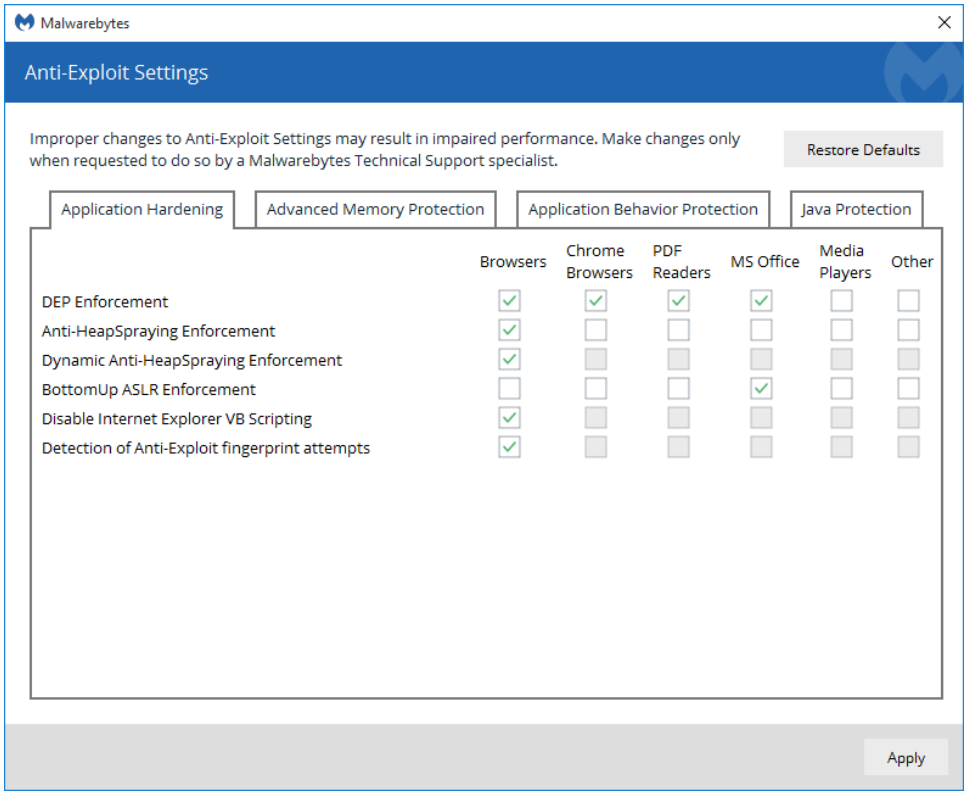
Many popular applications have been pre-configured for shielding. A screenshot is shown above. To change the status of any application, either use the Protection slider, or double click either the Application or File Name. Premium/Premium Trial users may add protection for other applications, and edit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



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/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.



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.

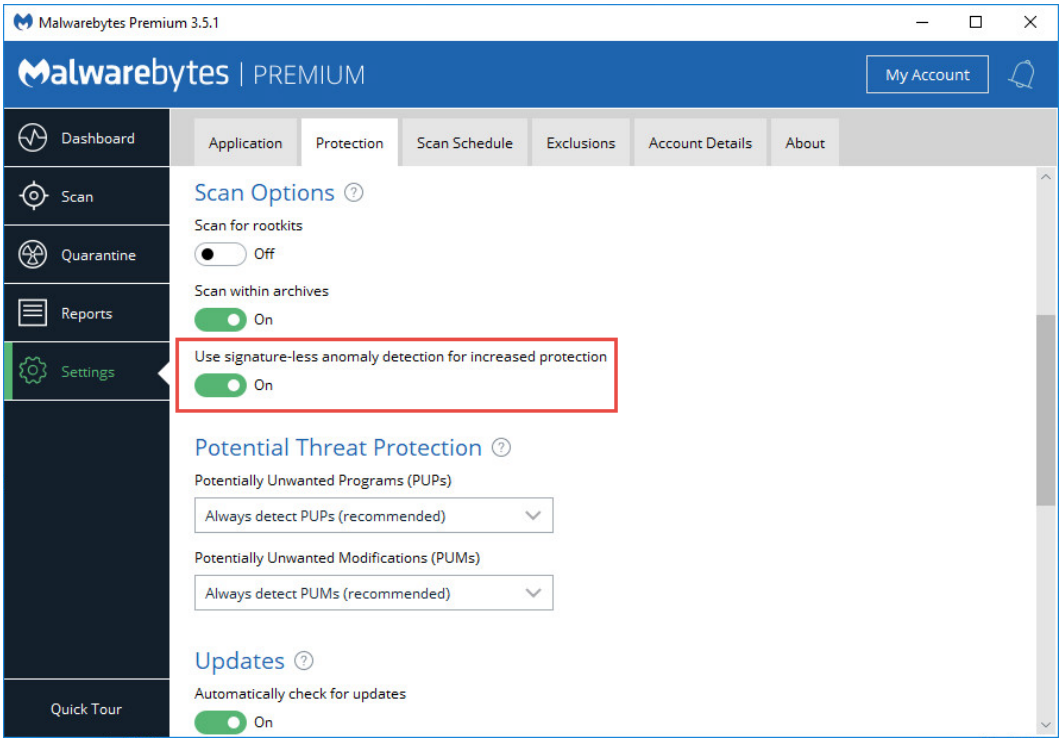
Malware Protection may be turned on or off as needed by Premium/Premium Trial users. It is on by default. This feature protects against malware present in code/files that try to execute on your computer. These files may have been downloaded, imported from a USB drive, or received as an email attachment. 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/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* will scan two 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.



We have introduced a new detection technology that uses machine learning to identify anomalous and malicious files. This signature-less technology supplements our existing detection methods.

Potential Threats

In addition to malicious software detection and elimination, *Malwarebytes* 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* 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* and *Malwarebytes Premium Trial* 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* 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* behaves when your computer starts. You may launch several applications at startup, and they may initiate processes which require *Malwarebytes* launch timing to be adjusted. Let's look at each setting in detail.

- **Start Malwarebytes at Windows startup:** If this setting is unchecked, *Malwarebytes* 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*.
- **Delay Real-Time Protection when Malwarebytes starts:** There may be times when the startup of system services used by *Malwarebytes* 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* 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.

Automatic Quarantine

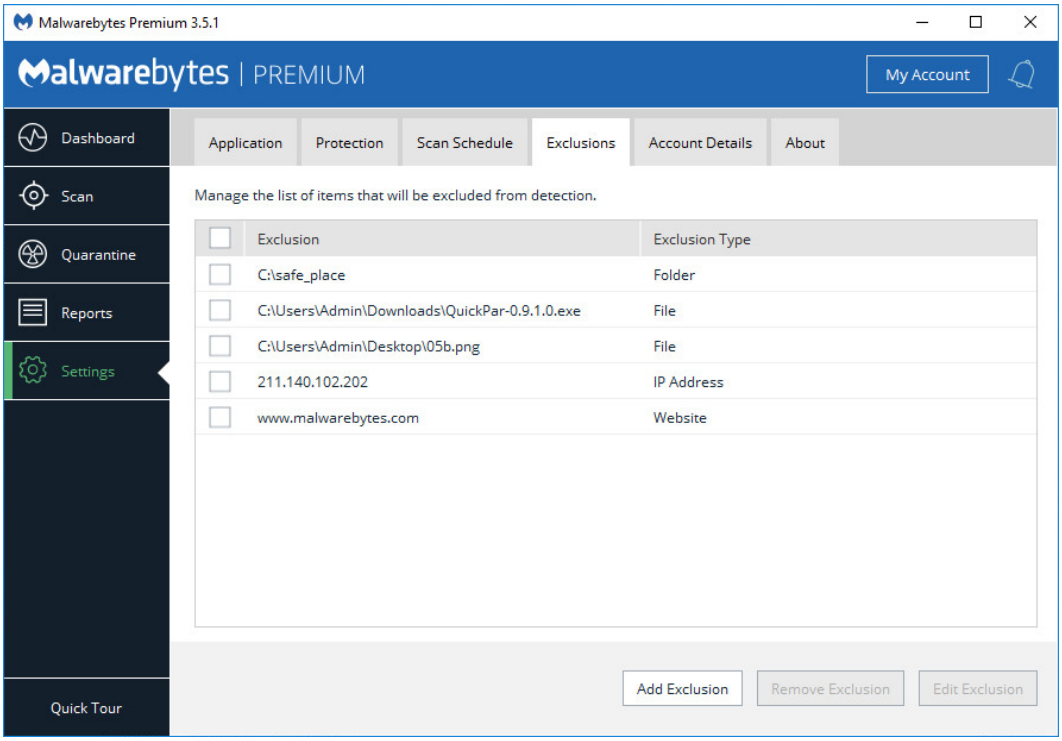
Users of *Malwarebytes Premium* and *Malwarebytes Premium Trial* may specify whether malware will be automatically quarantined when it is detected. The default setting is on. If the users decline to automatically quarantine malware, a notification will display in the lower right corner of the screen 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

You may also adjust Scan Schedules here as part of program settings. This aspect of program settings has already been covered on pages 11-19.

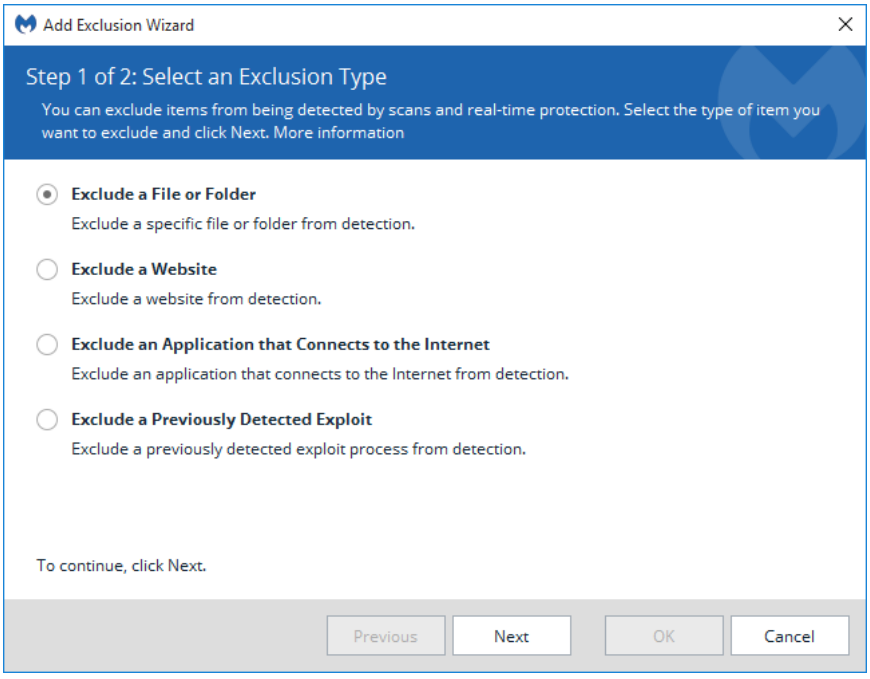
Exclusions

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.



Add Exclusion

Exclusions are exempt from scanning and from real-time protection. This may include files, folders, web sites, applications and safe programs which have been identified as exploits. Clicking Add Exclusion launches the Add Exclusion Wizard, as shown below.



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

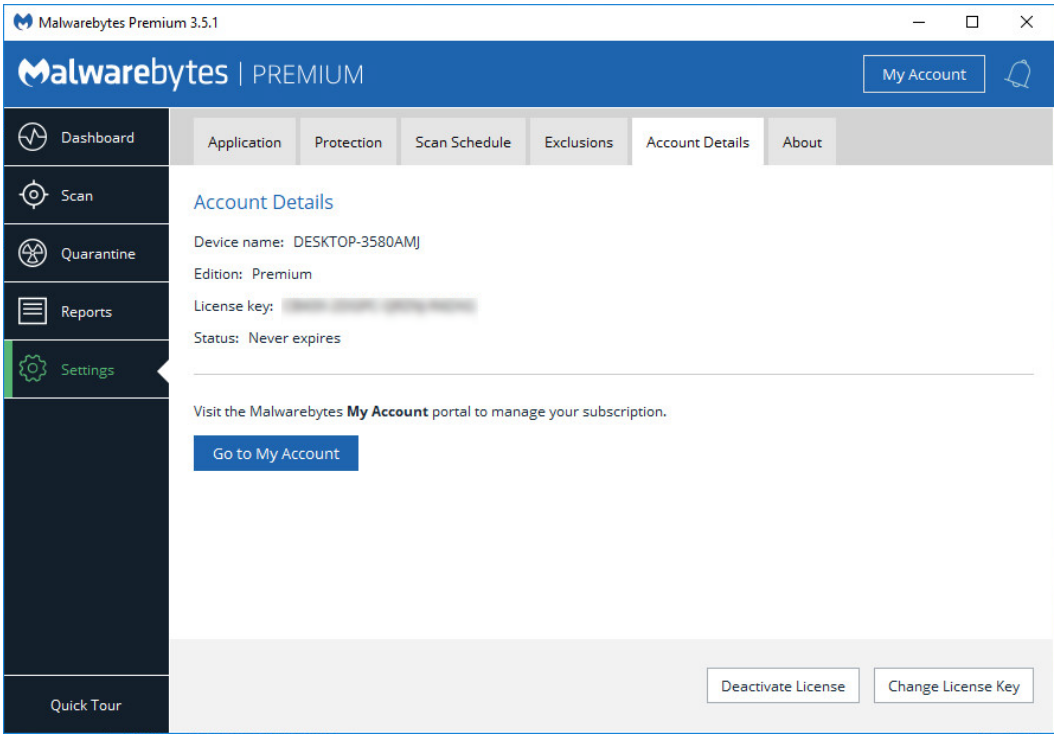
- **File or folder:** Its location on the file system, and whether it should be excluded from malware *and* ransomware, only malware or only ransomware. While you may have your own reasons for excluding files or folders from scans, the primary reason for doing so is to prevent potential conflicts with anti-virus software. *Malwarebytes* 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

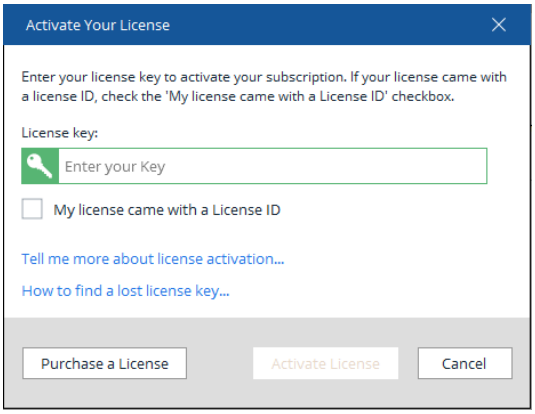
Here, you can click the **Go to My Account** button to obtain status of all of your subscriptions, and change preferences related to your account. You can also deactivate your license – useful when moving your Malwarebytes program to a new computer – or change license key. A screenshot is shown below.



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
Premium 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* 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 Premium 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** (Premium Trial or Free mode), you will see the following screen superimposed over the *Malwarebytes* interface.



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

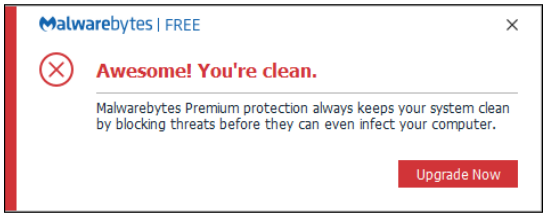
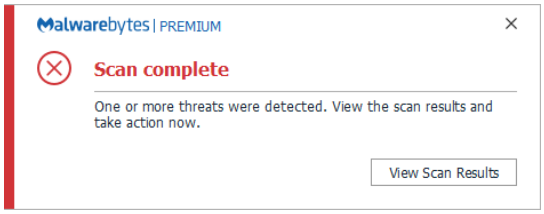
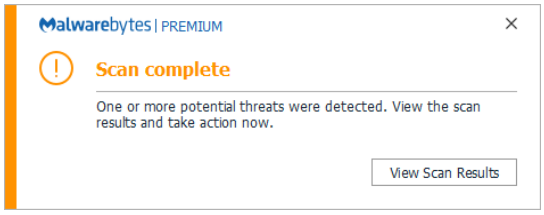
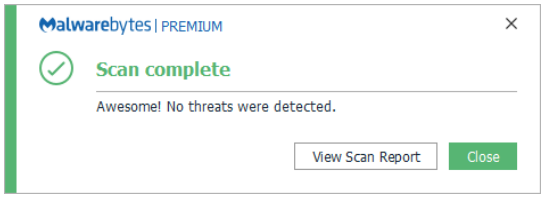
This tab tells you more about *Malwarebytes*, and what resources are available to you should you need technical assistance. The upper panel contains Version Information. We have split up the program into software components. If you have configured the program to provide program updates, it is easier 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).

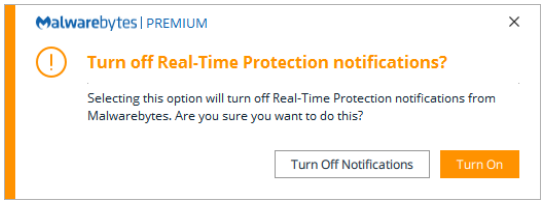
Appendix A: Notification Window Examples

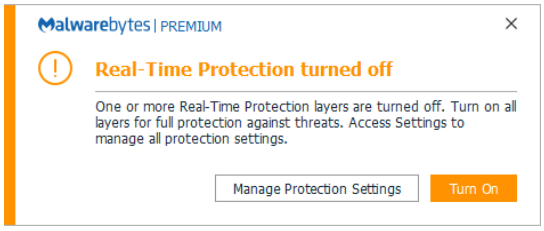
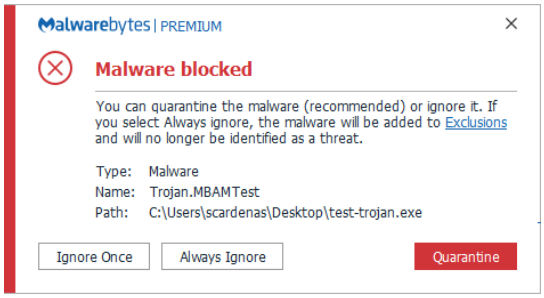
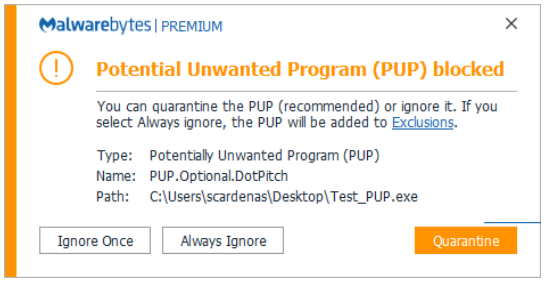
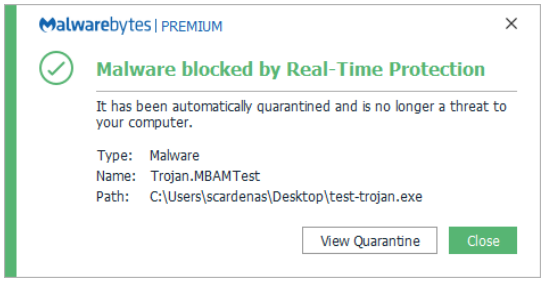
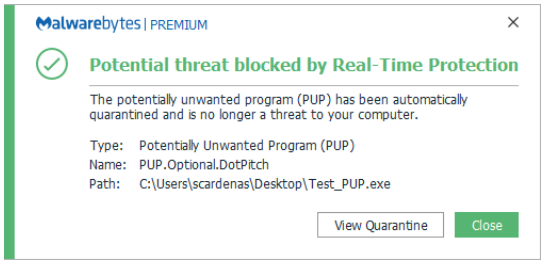
Malwarebytes provides a number of user notifications during operation. These notifications are always positioned in the lower right corner of your screen. The length of time that they will remain on your screen is configurable in *Application Settings* (page 24).

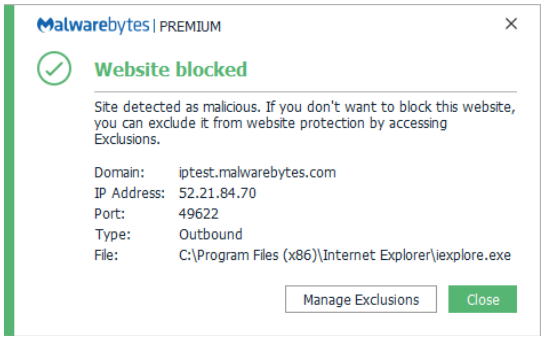
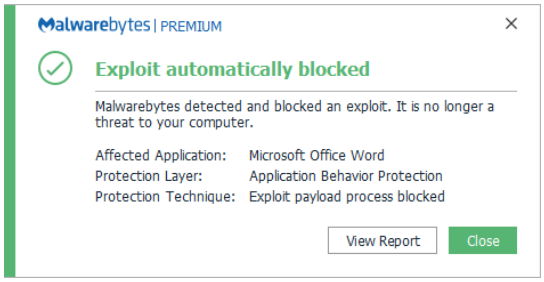
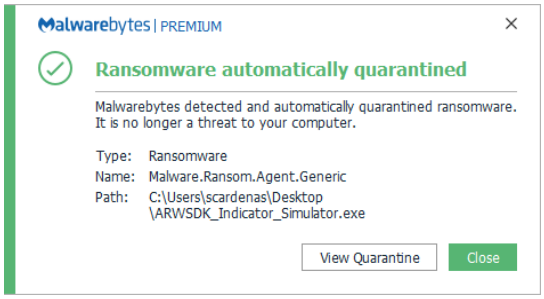
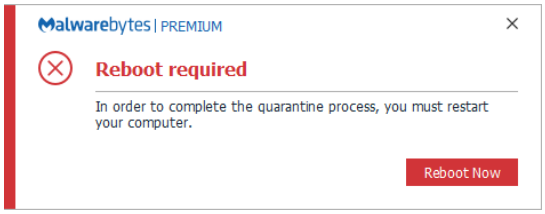
Scan Notifications

		An automatic scan has been completed. Malware was detected during execution of the scan. Click **Upgrade Now** to purchase *Malwarebytes Premium*. This notification will only appear for *Malwarebytes Free* users.
		A scan (scheduled or on-demand) has been completed. Malware was detected during execution of the scan. Click **View Scan Results** to review the scan log to determine the exact nature of the threat(s).
		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 **View Scan Results** to review the scan log to determine the exact nature of the threat(s).
		A scan (scheduled or on demand) has been completed. No problems were detected.

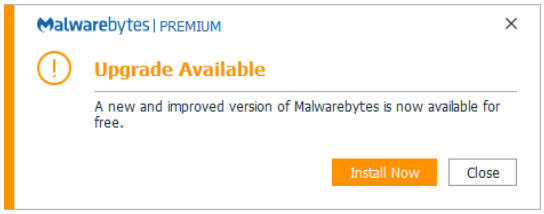
Real Time Protection Notifications

		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.

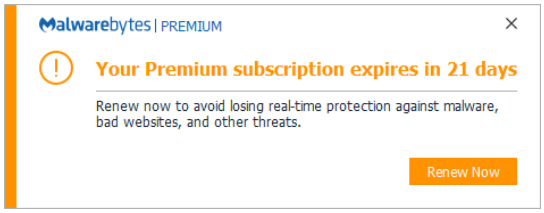
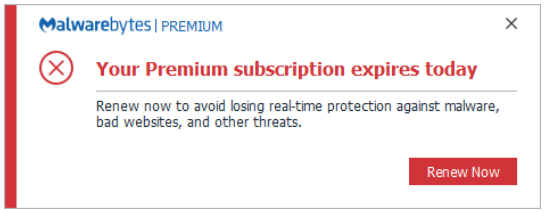
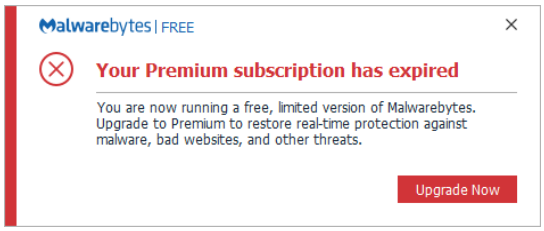
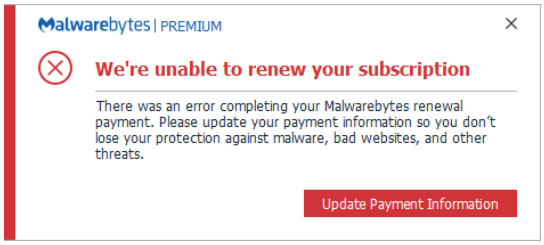
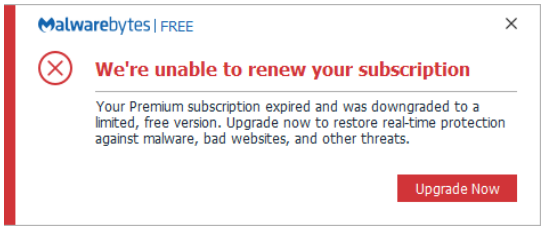
		One or more components of real-time protection are disabled. You may re-enable protection by clicking **Turn On** button, or by clicking **Manage Protection Settings**. This is not available for *Malwarebytes* free users.
		Malware has been detected as a function of real-time protection. You have not 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* users.
		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* users.
		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.
		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.

		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 **Manage Exclusions**, 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.
		Anti-exploit protection has prevented an attacker from exploiting your computer through a vulnerability.
		Anti-ransomware protection has prevented an attacker from exploiting your computer with suspected ransomware. The threat has been neutralized and moved to Quarantine.
		After threats have been quarantined, your computer must be rebooted to complete the quarantine process, and this notification is displayed. After assuring that other work is saved, click **Reboot Now** to perform that task.

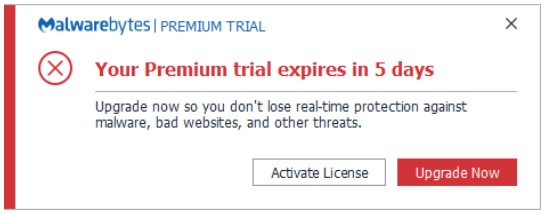
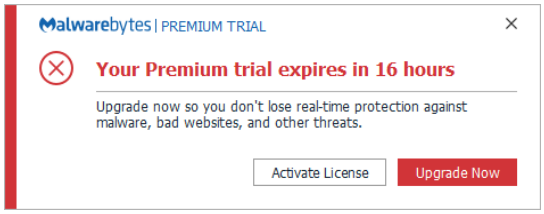
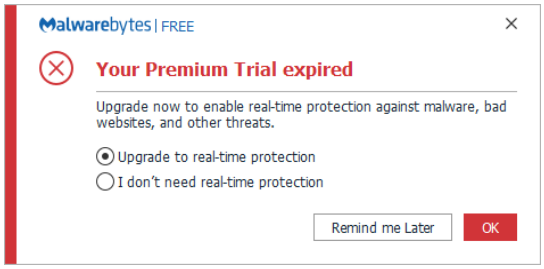
Update Notifications

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

Premium Notifications

		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. Click **Renew Now** button to renew your subscription in a new browser window/tab.
		If you do not have auto-renewal set up on your Malwarebytes account, this notification is displayed on the final day of your subscription. Click **Renew Now** button to renew your subscription in a new browser window/tab.
		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*. Premium features have been disabled. Click **Upgrade Now** to renew your subscription in a new browser window/tab. A slightly different version of this notification appears within the Malwarebytes user interface.
		This notification is displayed if your subscription cannot be renewed. Usually the reason for this is an expired credit/debit card. You will be given an opportunity to update your card information, and your subscription will remain in force for a brief period.
		Your subscription has expired and could not be automatically renewed. Your Malwarebytes service has been downgraded from Premium to Free. You can still run scans for protection, though real-time protection is no longer in force.

Premium Trial Notifications

		Beginning five days before your Premium trial expires, you will receive a notification once per day about the expiring trial, and be given an opportunity to upgrade to Premium or to enter your Premium license information.
		On the last day of your Premium trial, you will receive a single notification, and be given an opportunity to upgrade to Premium or to enter your Premium license information.
		After your Premium trial expires, you will receive this notification in the *Malwarebytes* user interface as well as in the Windows system tray.