



---

## **Malwarebytes for Mac User Guide**

Version 3.7

28 February 2019

---



## Notices

---

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

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

The Malwarebytes logo is a trademark of Malwarebytes. Apple and MacOS are registered trademarks of Apple, Inc. All other trademarks or registered trademarks listed belong to their respective owners.

Copyright © 2019 Malwarebytes. All rights reserved.

## 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

<b>What's New in Malwarebytes for Mac</b> .....	<b>1</b>
Improvements .....	1
Stability/Issues Fixed.....	1
<b>System Requirements</b> .....	<b>2</b>
End-User License Agreement (EULA).....	2
External Access Requirements.....	2
<b>Installation</b> .....	<b>3</b>
Activating Real-Time Protection .....	3
Additional Steps for macOS 10.13 (or higher).....	3
Installation Complete!.....	5
Free, Trial or Premium? .....	6
Purchase and Activation.....	6
Traditional Purchase and Activation.....	6
In-App Purchase and Activation.....	7
Program Updates .....	7
Uninstallation .....	8
<b>Mac Menu Bar Access</b> .....	<b>9</b>
Malwarebytes Menu .....	9
Malwarebytes Application Menu.....	9
About Screen.....	10
<b>Dashboard</b> .....	<b>11</b>
Status Pane.....	11
Real-Time Protection Pane.....	11
App Block .....	12
<b>Scan</b> .....	<b>13</b>
Watching Scan Progress .....	13
Scan Results .....	14
<b>Quarantine</b> .....	<b>15</b>
Remediation and Restarts.....	15
<b>Reports</b> .....	<b>16</b>
<b>Settings</b> .....	<b>17</b>
General .....	17
My Account.....	18
Scheduled Scans.....	19

# What's New in Malwarebytes for Mac

---

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

## Improvements

---

- Added new App Block feature as an added layer of real-time protection
- Added other detection engine improvements
- Improved behavior for business users

## Stability/Issues Fixed

---

- Minor bug fixes and improvements

# System Requirements

---

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

- **Operating System:** macOS 10.10 or later.
- **Security & Privacy:** Allow apps to be downloaded from Mac App Store and identified developers (default setting)
- **Active Internet Connection**

## End-User License Agreement (EULA)

---

Use of this product is governed by our End-User License Agreement (EULA). This agreement may be viewed in its entirety at the following URL:

<https://www.malwarebytes.com/eula/>

## External Access Requirements

---

If you utilize a firewall or other access-limiting device, you must grant access for *Malwarebytes* to reach Malwarebytes services. These are:

<a href="https://data.service.malwarebytes.org">https://data.service.malwarebytes.org</a>	Port 443	outbound
<a href="https://data-cdn.mbamupdates.com">https://data-cdn.mbamupdates.com</a>	Port 443	outbound
<a href="https://*.mwbsys.com">https://*.mwbsys.com</a>	Port 443	outbound

# Installation

---

Installation of *Malwarebytes* is straight forward. Double-click the Malwarebytes installation file which you downloaded to start the installation process. Individual screens will be displayed for:

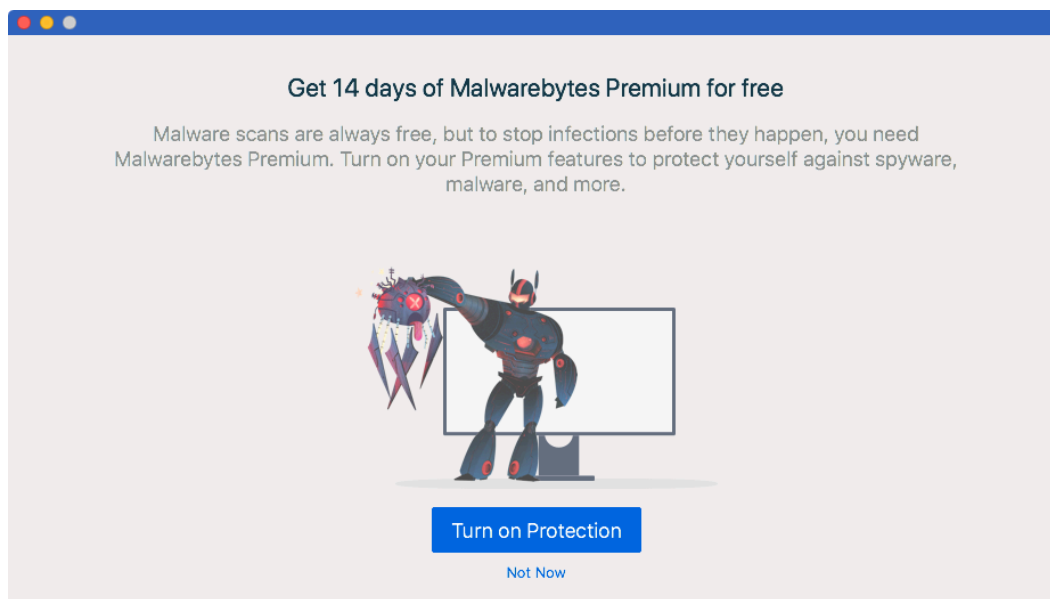
- **Introduction:** A reminder that bad things can and do happen to Macs
- **Read Me:** A rundown of changes between *Malwarebytes 3.0.3* and the previous version.
- **License:** The dreaded software license agreement
- **Destination Select:** Where should *Malwarebytes* be installed to?
- **Installation:** Admin privileges are required for certain parts of this installation.
- **Installation Type:** You can customize the installation to your needs.
- **Summary:** You're done! Now the fun begins.

The *Malwarebytes* installer now prompts you to select whether you will be using *Malwarebytes* in a Home or Business setting. This allows you to access a user interface adapted for a business experience, and helps make you aware of our business products, some which may be better suited to your protection in a business environment.

## Activating Real-Time Protection

---

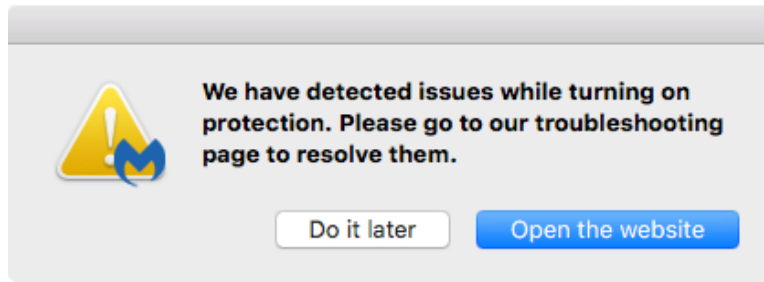
Once installation finishes, you will see the screen shown here.



Click **Turn On Protection** to activate Premium features. Users of macOS 10.13 (or higher) should read the next section as well.

### Additional Steps for macOS 10.13 (or higher)

Beginning with High Sierra, additional steps are required to complete installation. After clicking **Turn on Protection**, you will receive additional notifications. The first notification informs you of a catastrophic error that prevents real-time protection from being enabled. It is shown here.



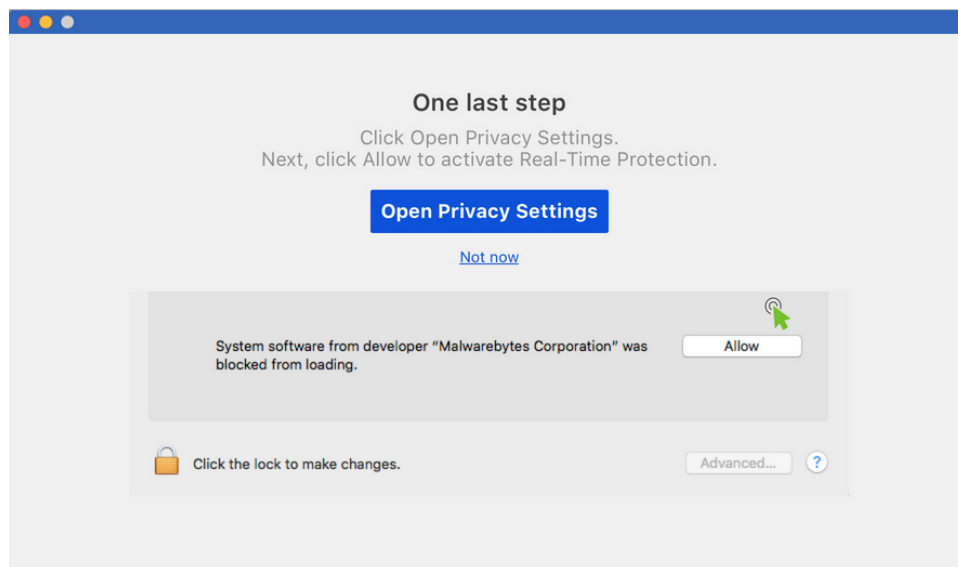
Should you get this notification, click **Open the website** to get further instructions. You will be directed to the following knowledge base article on the Malwarebytes Customer Success website:

<https://support.malwarebytes.com/docs/DOC-2632>

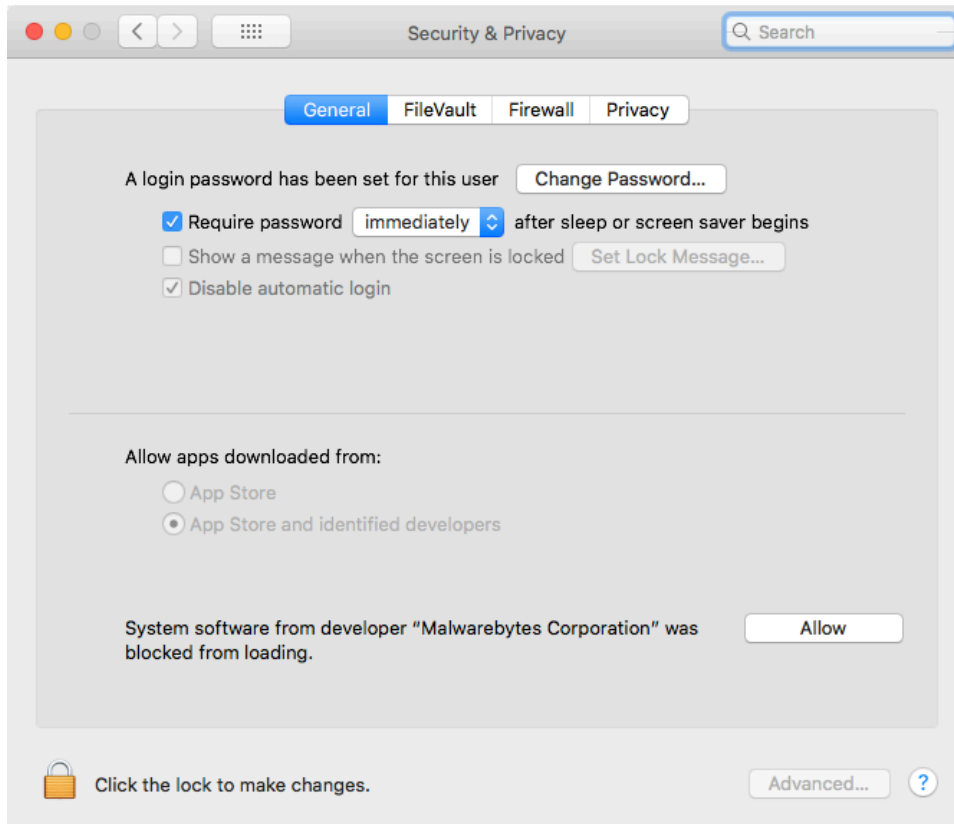
Normally, you will see the following notification, which will inform you that a system extension was blocked.



Click **OK** to display the window shown below, then click **Open Privacy Settings** to make changes necessary for *Malwarebytes* to function fully on the computer.



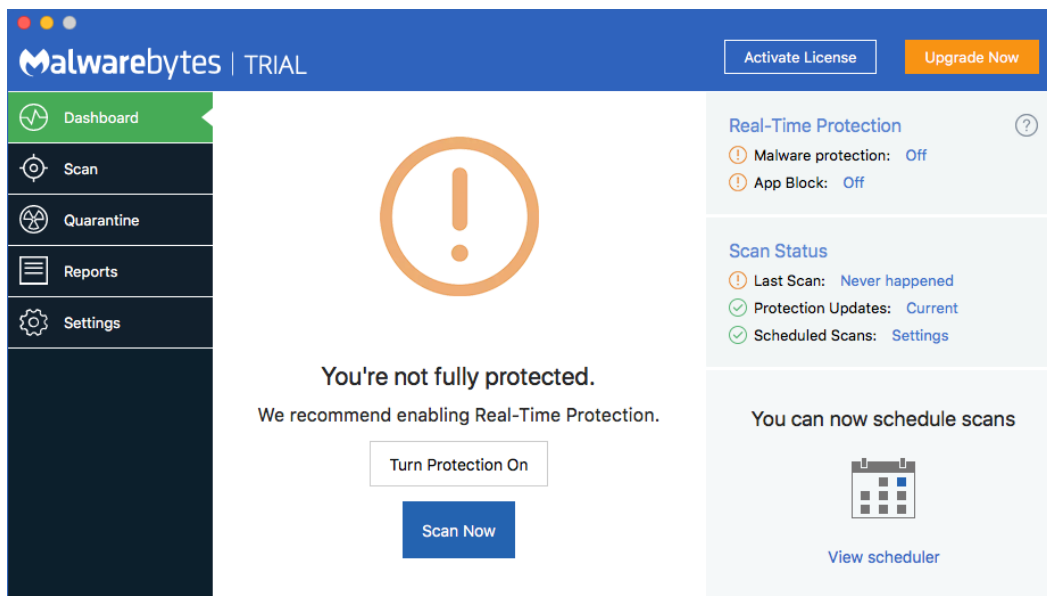
Click **Allow** (in the lower part of this window) to give *Malwarebytes* its full capabilities, then close the window.



You will be returned to *Malwarebytes*, confirming that real-time protection is now active. Click **Done** to begin using the program.

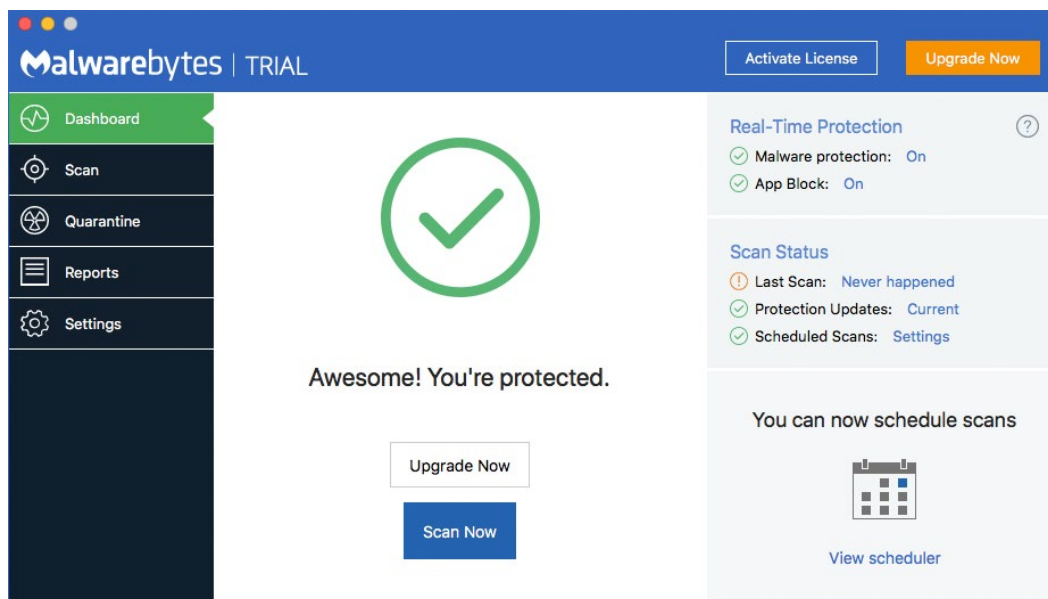
## Installation Complete!

At this point, program installation is complete. When you open *Malwarebytes* for the first time, one of the next two windows will be displayed. The first window indicates that you have not enabled *Malwarebytes* system extensions, preventing it from loading properly. Click **Turn Protection On** to return to the previous step and complete this process.





The next window is displayed if *Malwarebytes* is fully enabled to protect your computer. 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. That is covered on the next page of this guide.



## 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*. This may be unfamiliar territory for new *Malwarebytes* users. Here is a basic rundown on the differences between the Free and Premium versions of *Malwarebytes*.

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 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.

## Purchase and Activation

*Malwarebytes* is available for users of any modern Mac client to download and install at no cost to them. They can also purchase a subscription, which entitles them to take advantage of real-time protection and update scheduling. 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** will assist you in purchasing a license and unlocking the full potential of *Malwarebytes*. This can take one of two forms, which will be explained here.

### Traditional Purchase and Activation

When clicking **Upgrade Now**, most users will see a browser window that takes them to the *Malwarebytes* web site to purchase a license. Once the purchase has been made, license information will be sent to you in an email. Locate your license information and click the **Activate License** button. **Please note:** You must be online with an active Internet connection in order to successfully activate your Premium license.

Enter your license key to activate your subscription.

License key:

[Purchase a License](#) [Activate License](#) [Cancel](#)

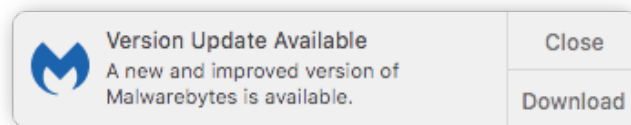
If you do not already have a license key, click **Purchase a License** to purchase one from the Malwarebytes website. After entering your license information, click **Activate License**. The two license-related links in the Menu Bar have been replaced by a link called **My Account**. Also note that the [License](#) has changed from *Malwarebytes Trial* to *Malwarebytes Premium*.

## In-App Purchase and Activation

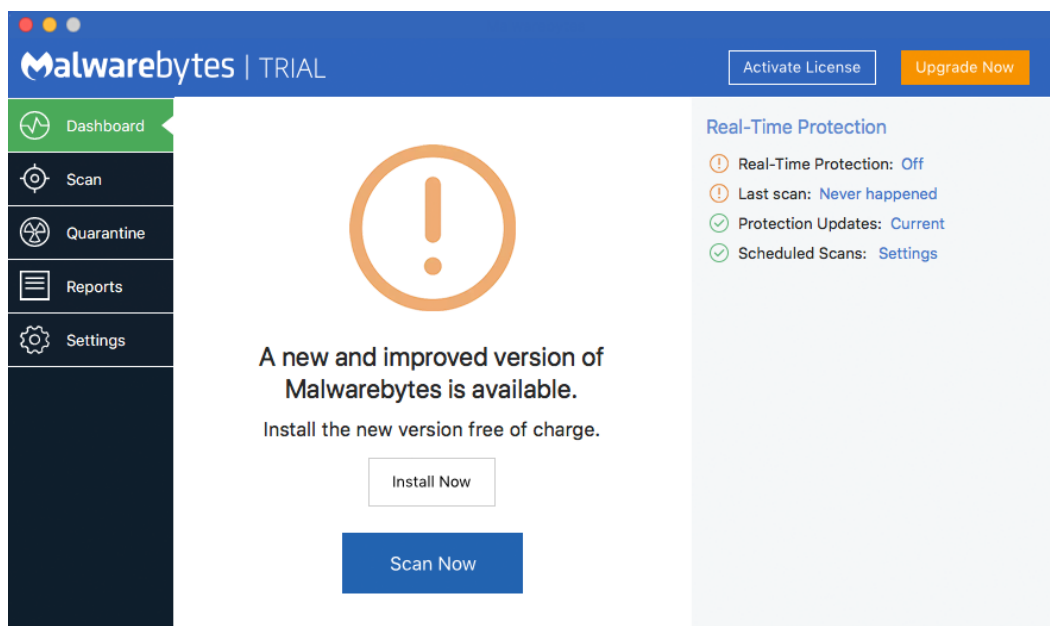
Users in some countries may be able to utilize a newer process which uses a “helper” screen before going to the web site to purchase a license. It will launch when clicking **Upgrade Now**. Following the license purchase, the license key will be inserted into the activation screen automatically. When you see the license displayed, click **Activate License**. **Please note:** If a license cannot be provided, you will receive further instructions at that time.

## Program Updates

*Malwarebytes* automatically checks to determine if a new version is available. If an update exists, the following notification appears in the upper-right corner of your screen.



Click **Close** to dismiss the notification, or click **Download** to download the latest *Malwarebytes* version onto your system. To install the update, you will need to relaunch *Malwarebytes* once the download has completed. The update will be available on the Dashboard, as shown below.



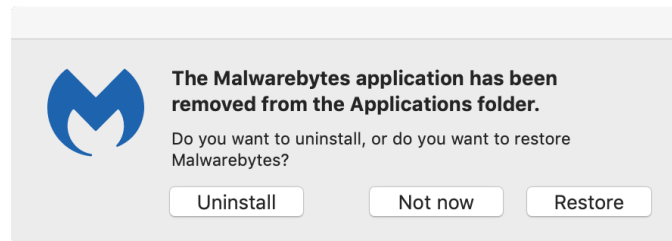
Click **Install Now** to perform the installation.

## Uninstallation

---

Should you ever need to uninstall *Malwarebytes* from your computer, you will find an option to perform this task in the [Help](#) menu. Please note that admin rights for the computer will be required to perform this task.

If you remove *Malwarebytes* from the Applications folder, the application will ask you to confirm whether you meant to uninstall it. You can click to **Uninstall**, or **Restore** the application. If you want to leave things how they are, you can click **Not now**.

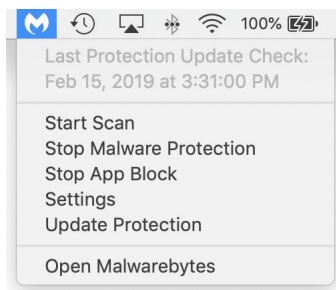


# Mac Menu Bar Access

Access to *Malwarebytes* is available to the user from two different access points on the Mac Menu Bar. They are as follows:

## Malwarebytes Menu

The *Malwarebytes* menu is visible in the menu bar at all times, and is represented by the *Malwarebytes* icon in the right side of the menu bar. Click on the *Malwarebytes* icon to launch the following screen directly below the menu bar. Descriptions of the settings are shown below as well.



- **Last Protection Update Check** is an informational display to let you know when the most recent database update check occurred, and updated (if an update was available).
- **Start Scan** initiates a Threat Scan.
- **Stop Malware Protection** disables real-time protection against malware on the hard drive. When stopped, the option changes to **Start Malware Protection**.
- **Stop App Block** disables the App Block protection feature. When stopped, the option changes to **Start App Block**.
- **Settings** launches the Settings screen. This will be discussed on page 15 of this guide.
- **Update Protection** causes an immediate database update.
- **Open Malwarebytes** launches the *Malwarebytes* app.

## Malwarebytes Application Menu

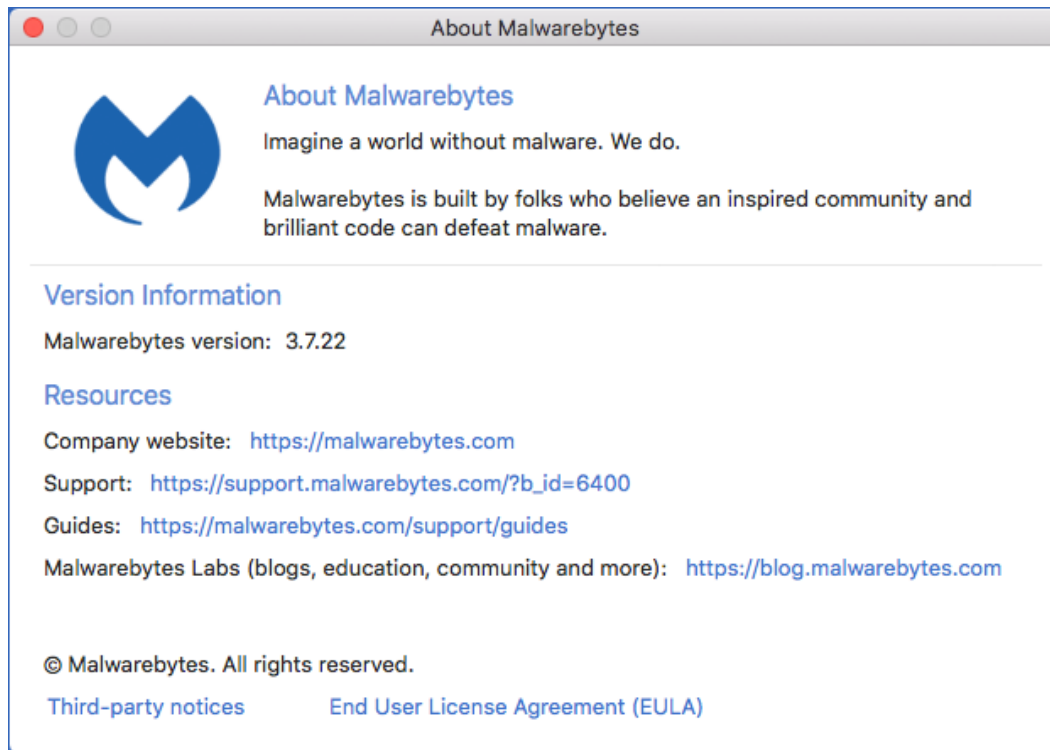
The Malwarebytes Application menu is visible only when the *Malwarebytes* app is open and in front. It is a standard Mac feature. Options shown on this menu are as follows:



- **About Malwarebytes** shows the About screen (shown below).
- **Preferences** displays the Settings screen (as shown earlier).
- **Services** allows use of Mac services that apply to the current app.
- **Hide Malwarebytes** hides the *Malwarebytes* program interface.
- **Hide Others** hides all screen content except for the *Malwarebytes* interface.
- **Show All** unhides content which had been hidden by **Hide Others**.
- **Quit Malwarebytes** terminates the *Malwarebytes* interface, while real-time protection remains active (unless it has been disabled).

## About Screen

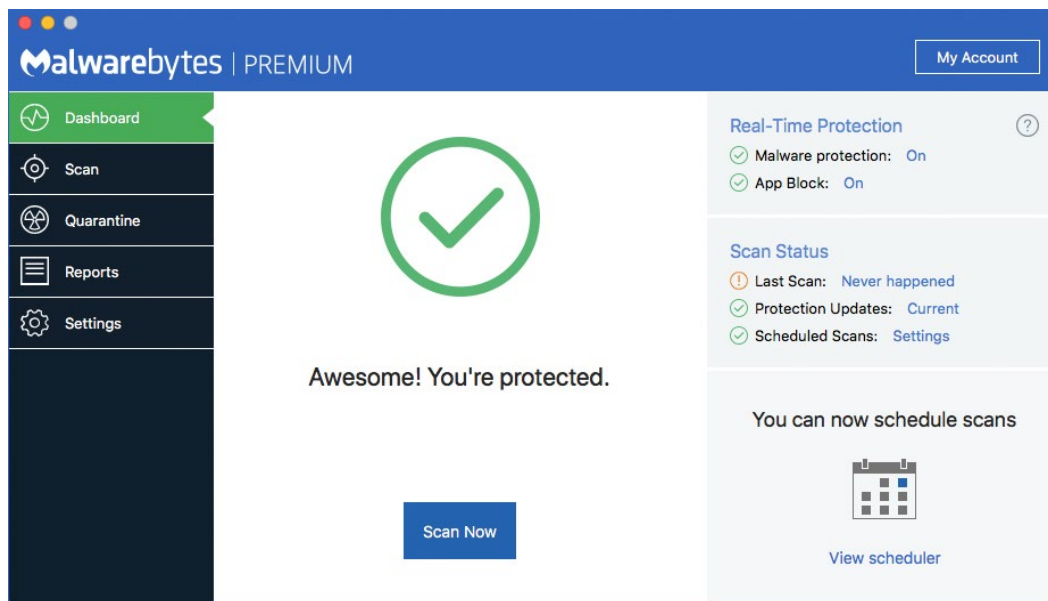
This screen tells you more about *Malwarebytes*, and what resources are available to you should you need technical assistance. A screenshot is shown below.



The upper panel contains Version Information. The Resources section provides contact addresses (URLs) which may offer assistance 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).




# Dashboard

Each time *Malwarebytes* 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.



## Status Pane

The main area of the screen is the Status Pane, providing current system status. The first item displayed in system status is always the severity level. Severity levels are shown here:

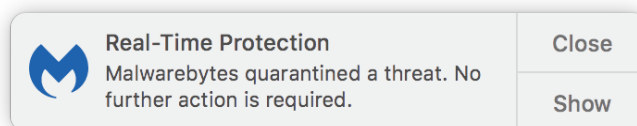
		
<b>Critical:</b> Immediate attention is required.	<b>Warning:</b> Please take action before the situation becomes critical.	<b>OK:</b> No problems noted.

There are many variations in the message and sub-message which may be presented for each severity level.

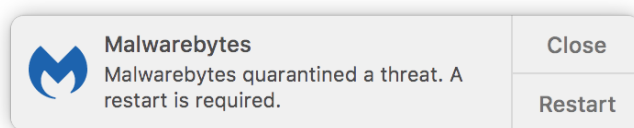
## Real-Time Protection Pane

This pane shows whether Real-Time Protection is on or off, when the last scan was executed, and the status of your protection database. If you are in Trial mode, Real-Time Protection is enabled unless you turn it off. **Please note** that Real-Time Protection is enabled only for *Malwarebytes Premium* and *Malwarebytes Trial* users. This feature is not available if you are using the Free version.

You may encounter threats while performing your everyday tasks. When Real-Time Protection is enabled, a threat would trigger the following notification in the upper right corner of your screen.



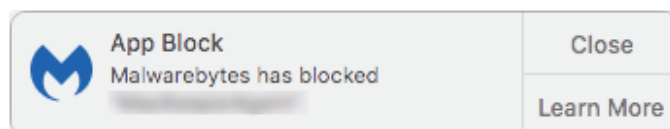
If you click **Close**, the notification will be dismissed. Click **Show** to launch the *Quarantine* screen, as shown on page 14. There may also be instances when real-time protection quarantines a threat and determines that a restart is necessary to remediate the threat fully. That notification looks very similar. It is shown here.



When a restart is required, please remember to save all work before clicking **Restart**.

## App Block

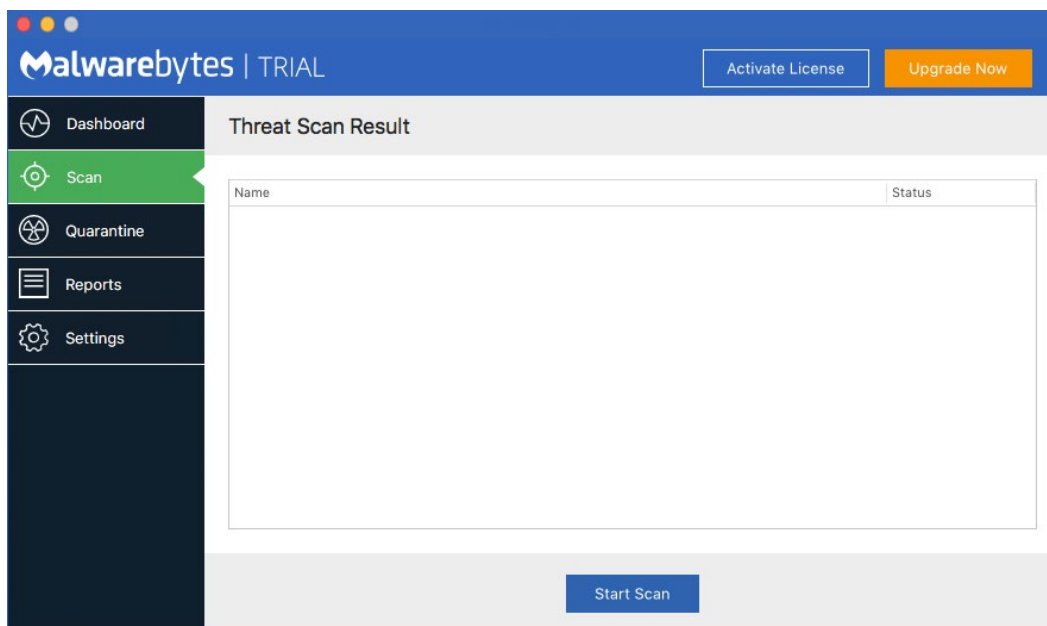
We have added a new feature called App Block. Its purpose is to proactively block execution of apps that originate from known bad developers, regardless of whether we have seen the app before or not. A blocked app is not deleted or quarantined in any way, only prevented from executing on your computer. Here is a screenshot of the App Block notification you will see if the protection feature is triggered.



Malware protection and App Block can be enabled or disabled individually, but clicking **Turn Protection On** on the Dashboard will enable both forms of protection.

# Scan

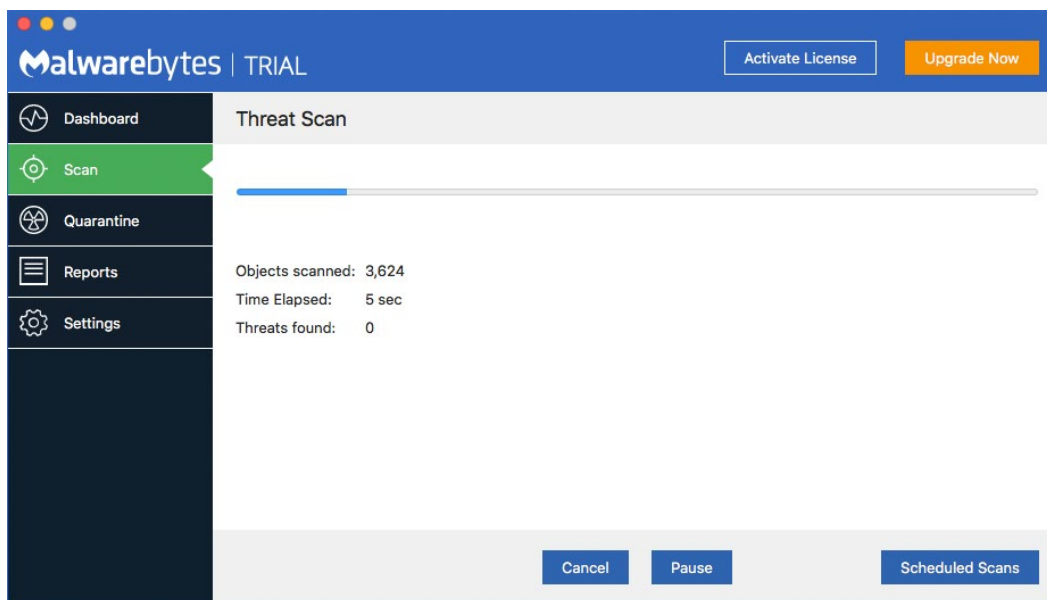
The **Scan Pane** allows you to run a Threat Scan on your computer. You may run a scan at any time. If you are familiar with *Malwarebytes* scanning methods, the program executes a Threat Scan. That method checks all locations on your computer which are commonly used for storage and launching of malware. A screenshot is shown below.



Click **Start Scan** to initiate a scan.

## Watching Scan Progress

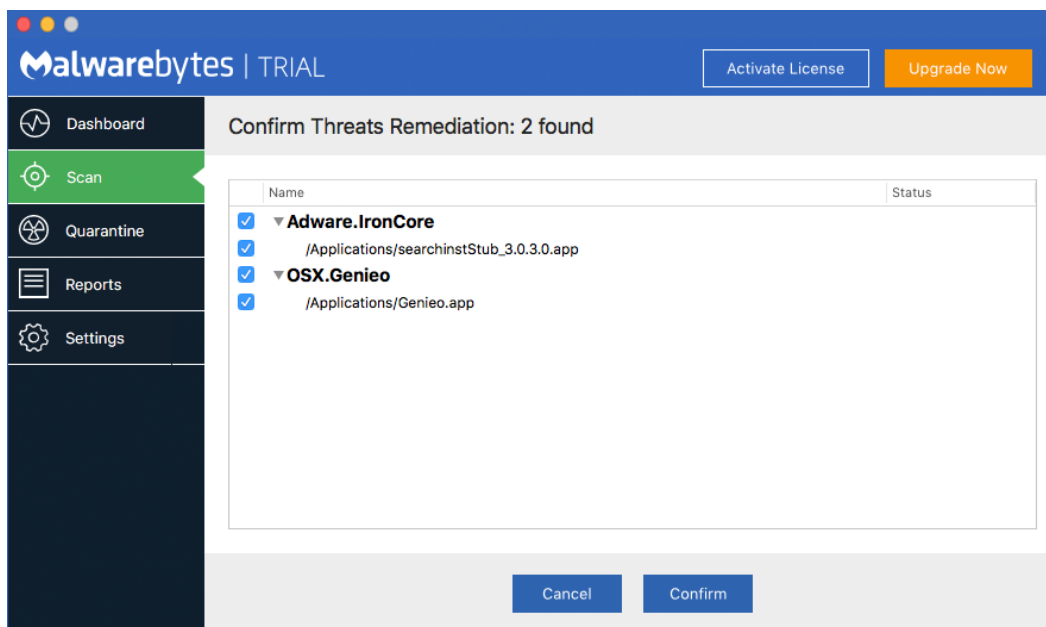
Threat Scans on a Mac execute very quickly. This is normal, and not a cause for alarm. Should you feel so inclined, the following screenshot shows a scan in progress.





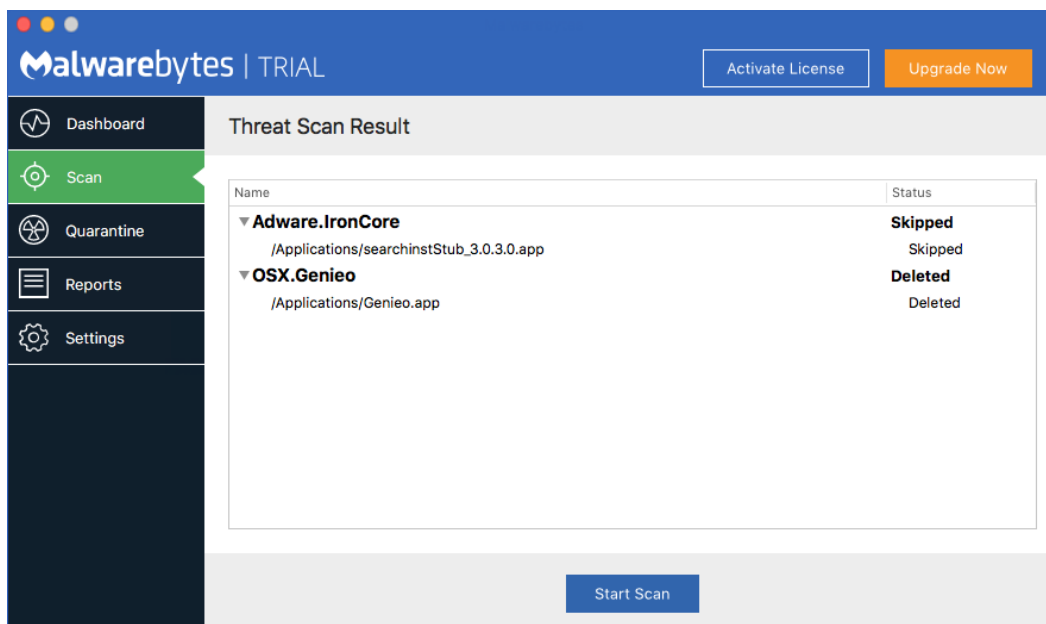
## Scan Results

If threats are detected during the scan, a count of detected threats is displayed. More detailed threat information is displayed after the scan completes.



You may note that the screen shown here says that two threats were found, while it appears that four items are shown. The items shown in bold are the names of the threats themselves, while the information immediately below the threat name is a component of the threat. Threats may have several components. When that is the case, they will all be displayed.

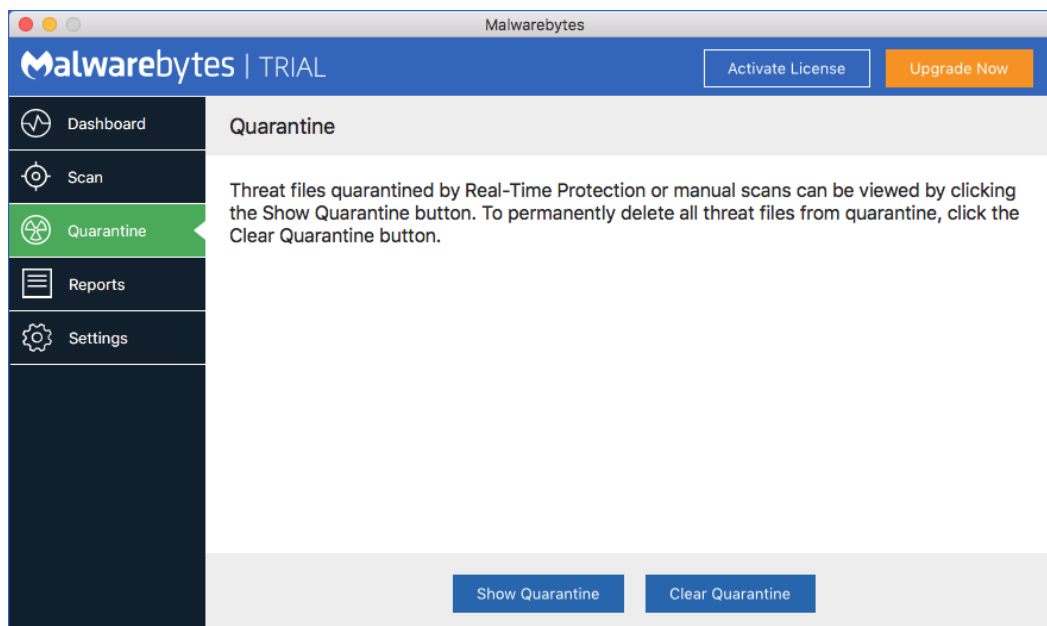
You may click **Cancel** to skip further processing of the detected threats. You may also uncheck threats you do not wish to remove, then click **Confirm**. Using the above screen as a reference, if we uncheck *Adware.IronCore* (the first threat) and click **Confirm**, we will be presented with the following screen.



Threats which have been moved into Quarantine cannot harm your computer. They are neutralized as part of the Quarantine process, and can be processed further at any time.

# Quarantine

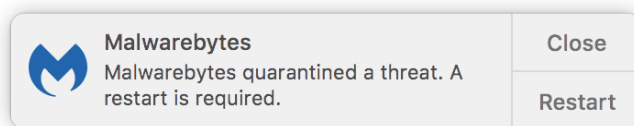
When you run a scan, detect threats and authorize their removal, they are moved to a special *Malwarebytes* folder called **Quarantine**. When real-time protection detects a threat, that threat is also moved to the Quarantine folder. If you want to inspect the contents of the Quarantine folder, click **Show Quarantine** on the Quarantine screen. A screenshot is shown here.



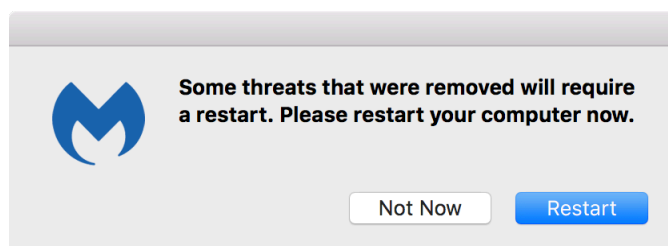
That will open a new system window showing the contents of the Quarantine folder. That system window is only there for your inspection. If you wish to delete the contents of the Quarantine folder, you should click **Clear Quarantine** in the *Malwarebytes* Quarantine screen. You will be presented with a confirmation window before the deletion takes place.

## Remediation and Restarts

Sometimes your computer must be restarted to complete remediation of threats that were detected. Restarts necessitated by real-time protection detections will show the following notification.



If a restart is required to complete remediation of threats detected during a scan, the following notification is shown instead.

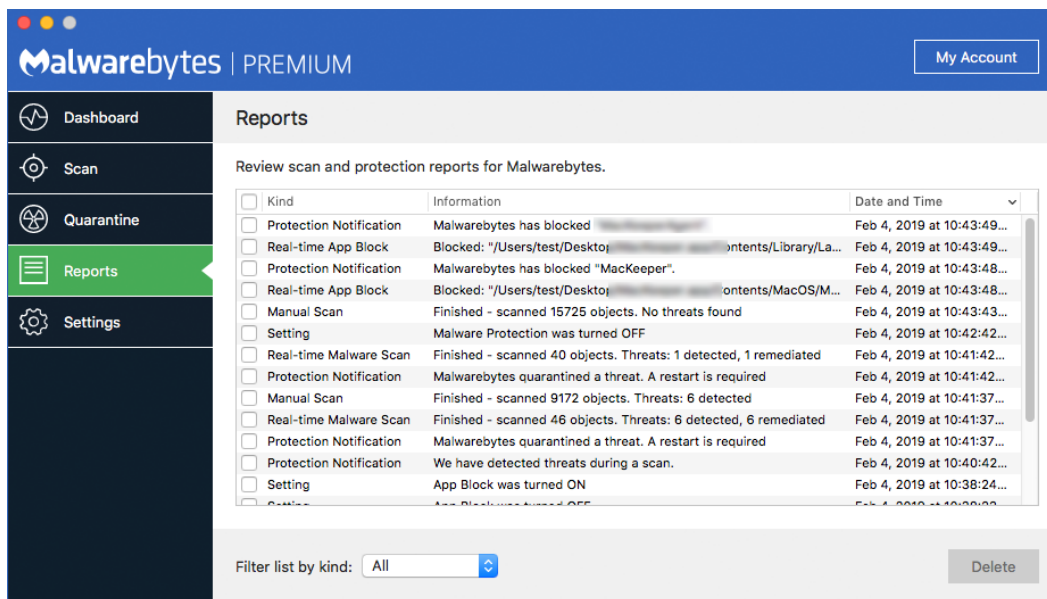


When a restart is required, please remember to save all work before clicking **Restart**.

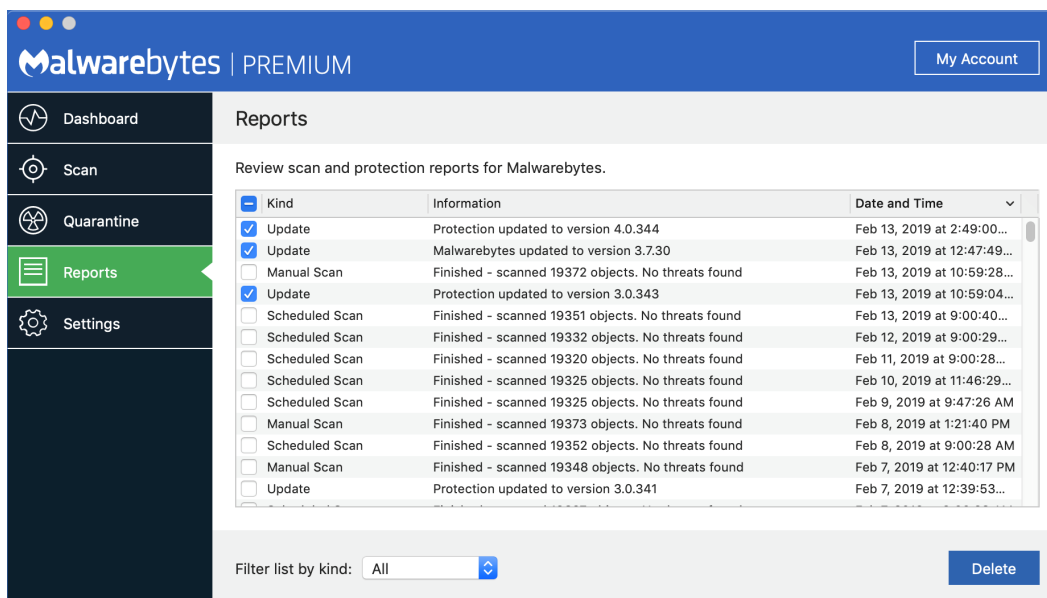
# Reports

Malwarebytes saves records of events that occur in the application. You can review these by clicking the [Reports](#) button on the left side of the interface. The following event categories are saved to Reports.

- Scans
- License Status
- Setting changes
- Program and/or Protection Updates
- Notifications
- Real-time App Blocks



You can sort the events in Reports using the Date and Time – Click the header to change the sort order. The menu at the bottom of the interface allows you to filter the category of Report shown. The checkbox to the left of each entry allows you to delete events. You can quickly select or deselect all events by clicking the top-most checkbox. **Delete** will become active once you have selected one or more events. Over time, Malwarebytes automatically deletes older report events to make room for new entries.



# Settings

---

Program settings (also known as *Preferences*) are available in three locations:

- The Malwarebytes Application menu, at the left edge of the Mac Menu Bar.
- The Malwarebytes menu, in the right portion of the Mac Menu Bar.
- From the Settings button on the left side of the *Malwarebytes* program interface.

Program settings are divided into three sections. Click **Settings** in the menu panel to access settings. The screen is divided into three sections – we will describe each of these below.

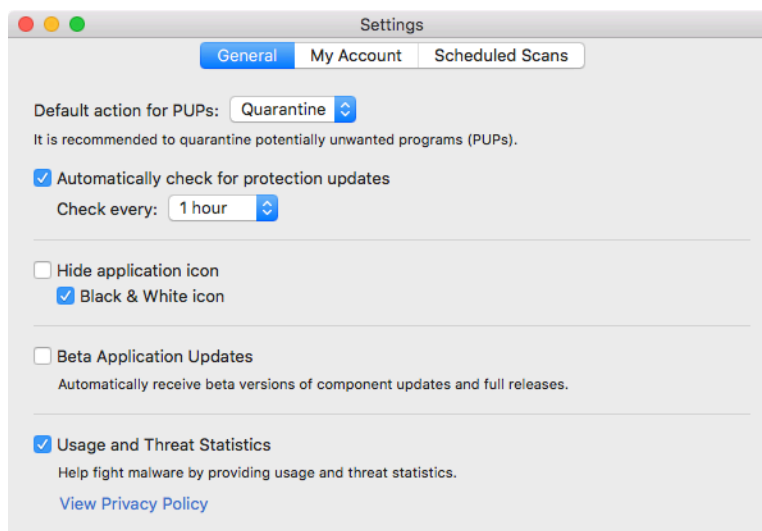
## General

---

The default tab when you open Settings is *General*. You will note that General is highlighted in blue, indicating it is the selected settings group. Available settings are:

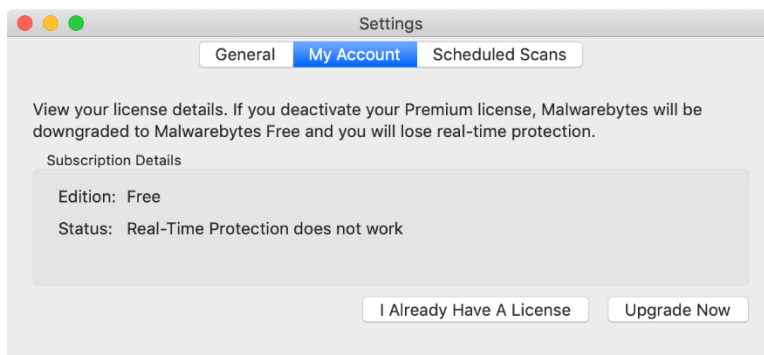
- **Default action for PUPs** determines the action taken on PUPs. The default option is to Quarantine PUPs, although you may also choose to Skip processing instead. This would exclude PUPs from scans. You may still quarantine PUPs by selecting them after a manual scan.
- **Automatically check for protection updates** may be selected or deselected. We strongly recommend that you select this option in order to benefit from the most current database updates. When selected, the **Check every** setting allows updates to be scheduled for once an hour (the default) up to once per 24-hour day (in 5 discrete steps).
- **Hide application icon** causes this icon in the menu bar to not be displayed. This setting is unchecked by default.
- **Black & White icon** will cause the application icon in the menu bar to be displayed in monochrome when selected, or in color when not selected. The default is Black & White (selected).
- **Beta Application Updates** will cause the application to download beta (pre-release) updates in addition to normal releases. This setting is unchecked by default. After enabling this setting, you will receive an additional screen to confirm your choice.
- **Usage and Threat Statistics** will cause the application to send anonymized data from the application to us for analysis. This data helps our researchers and engineers improve the product and help protect you. For a full list of information that is collected, please see the Malwarebytes Privacy Policy, at:

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

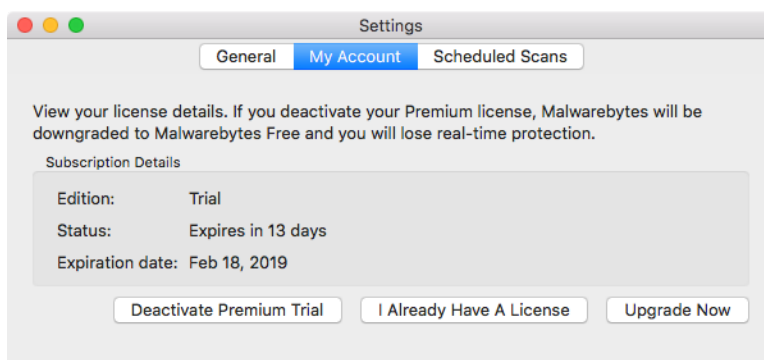


## My Account

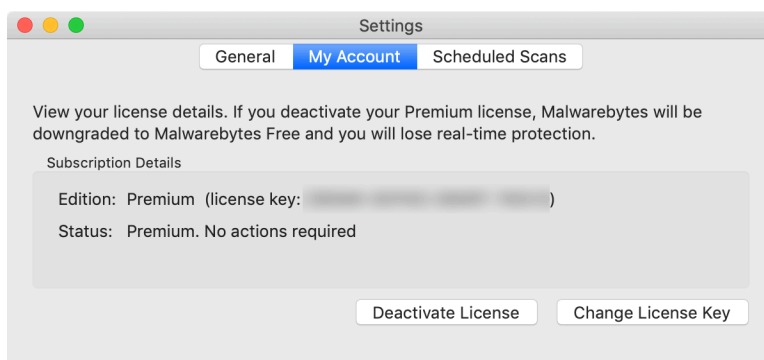
The *My Account* tab has three variations. The first variation is for Free users. This screen allows you to start a Premium Trial, enter a Premium License, or purchase a Premium license. You will only be able to start a Premium Trial if one is available to you.



The second variation is for Trial users. It offers the opportunity for the user to purchase a license, to enter a license that they have already purchased, or to deactivate the Trial. If you deactivate your trial, you will no longer be able to use Real-Time Protection, and you will not be able to resume the Trial at a later time.

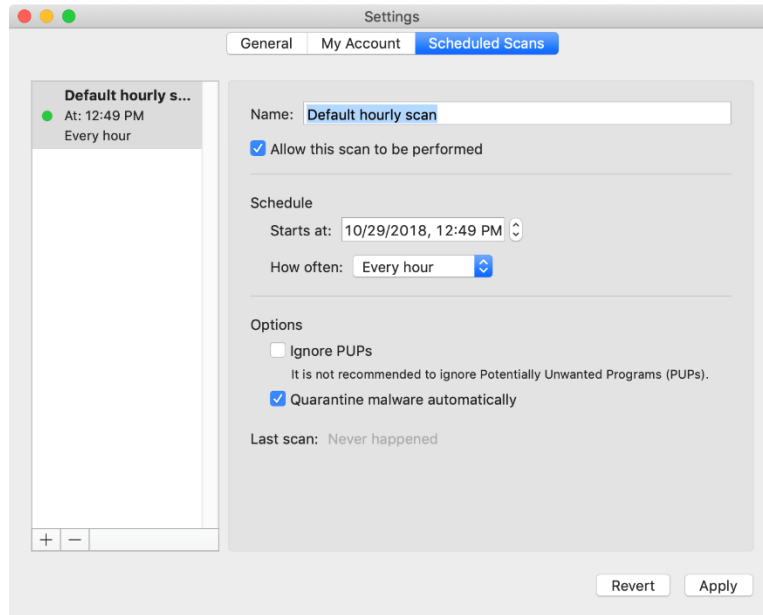


If you are using the Premium version of *Malwarebytes*, a slightly different screen is shown. This version takes into account that you have already purchased a license and will display your license key, should you require it. The three buttons at the bottom are replaced with the **Change License Key** button, and the **Deactivate License** button. The screen is shown here.



## Scheduled Scans

The final tab is *Scheduled Scans*. This tab allows you to configure *Malwarebytes* to run scans on a defined schedule. Scheduled scans help to provide more comprehensive protection on your device. Trial or Premium users may add and configure several scheduled scans simultaneously. Free users may only enable or disable a single, default scan.



The available options for Scheduled Scans are:

- **Name:** Provide a name for the scheduled scan to help organize it among any others you have.
- **Allow this scan to be performed:** Checking this box will enable the scheduled scan. If you do not want the scan to run, simply uncheck this box to maintain all other scan settings.
- **Starts at:** Select the time of date and time that you wish the first scan in the series to run
- **How often:** Select the frequency of the scan.
- **Ignore PUPs:** If you select this, PUPs will not appear in the scan results and *Malwarebytes* will take no action on them as part of the scheduled scan. This is not selected by default when adding a scheduled scan.
- **Quarantine malware automatically:** This option will allow the scheduled scan to perform a quarantine action on any malware found as part of the scan. You will not be able to review the files detected before the quarantine occurs. This is enabled by default when adding a scheduled scan.

You may add a new scheduled scan by clicking the + at the bottom left of the list of scan names. You may remove a scheduled scan by clicking the – button. If you are a Free user, you will only be able to use a complimentary monthly scan. You are able to change the scan day or time, and you may disable it, but you cannot change any other settings or create new scans. Trial and Premium users can create any number of scheduled scans.