Malwarebytes

Malwarebytes for Mac User Guide
Version 3.0.2
21 August 2017

Malwarebytes

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. Windows is a registered trademark of Microsoft Corporation. All other trademarks or registered trademarks listed belong to their respective owners.

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

What's New in Malwarebytes for Mac

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

Performance / Protective Capability

- Added Real-Time Protection for Premium/Trial users

Usability

- Added notification for detections by real-time protection
- Redesigned user interface for improved usability and consistency with Windows program version
- Menu bar access to many basic program functions
- Simplified installation process

Stability / Issues Fixed

- Numerous improvements to program code

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:** OS X version 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:

https://data.service.malwarebytes.org	Port 443	outbound
https://data-cdn.mbamupdates.com	Port 443	outbound
https://*.mwbsys.com	Port 443	outbound

Installation

Installation of *Malwarebytes* is straight forward. Begin by opening the *Malwarebytes* folder, then double click on the icon titled Install Malwarebytes 3.pkg. This will 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* 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.
- **Summary:** You're done! Now the fun begins.

At this point, program installation is complete. When you open the *Malwarebytes* app, you will see the user interface as shown below. If you have already purchased a license, you may wish to activate your copy of *Malwarebytes* 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.
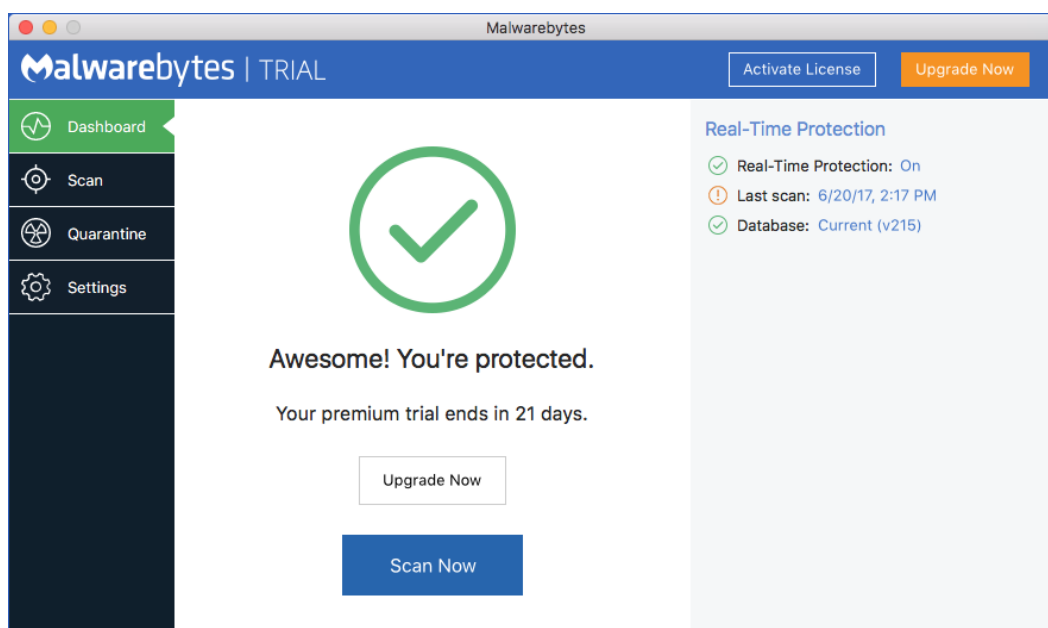
Free, Trial or Premium?

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 30-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.

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** launches a browser window which will take them to the Malwarebytes web site to purchase a license.

Your license information will be in an email sent to you by Malwarebytes at the time of purchase. Locate your license information and click the **Activate License** button. **Please note:** You must be online with an active Internet connection in order to successfully activate your Premium license. Please focus your attention to the top center portion of the screen shown below.
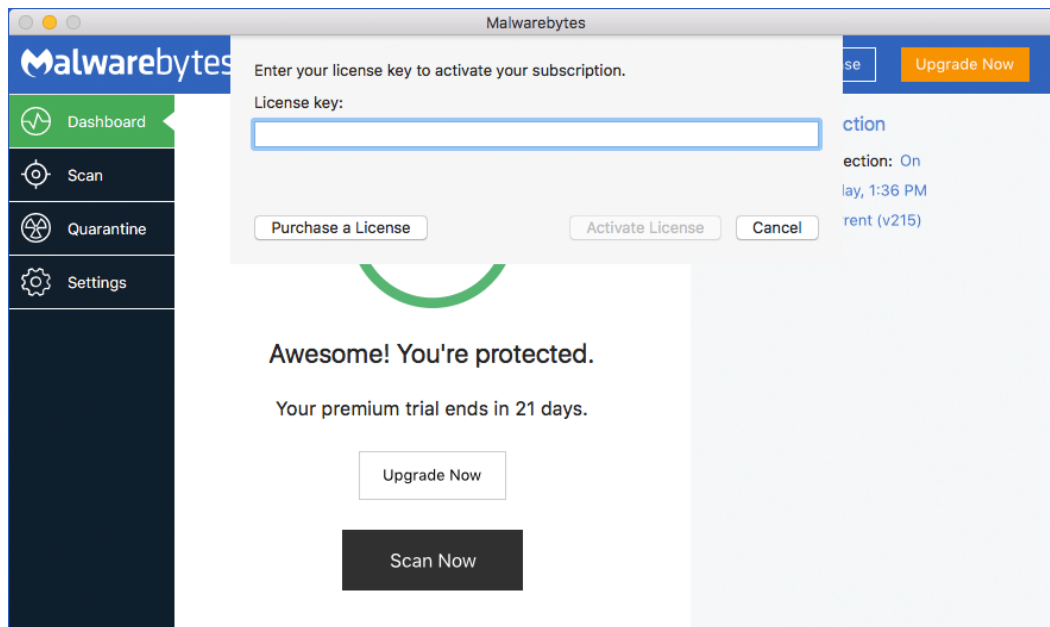

If you do not already have a license key, click **Purchase a License** to purchase one from the Malwarebytes website. After entering your license information, click the **Activate License** button. The two license-related links in the Menu Bar have been replaced by a link called **My Account**. Also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

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:
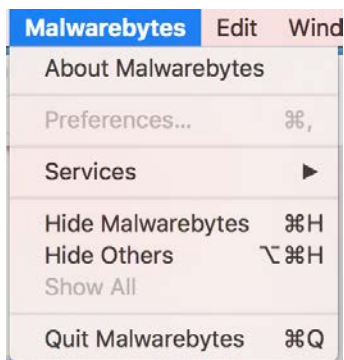
Malwarebytes Menu

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.
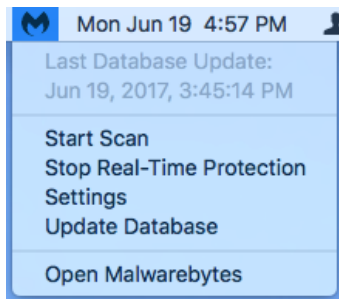
- Last Database Update is an informational display to let you know when the most recent database update occurred.
- Start Scan initiates a Threat Scan.
- Stop Real-Time Protection disables real-time protection. When stopped, the option changes to Start Real-Time Protection.
- Settings launches the Preferences screen. This will be discussed on page 11 of this guide.
- Update database 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, which is 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.
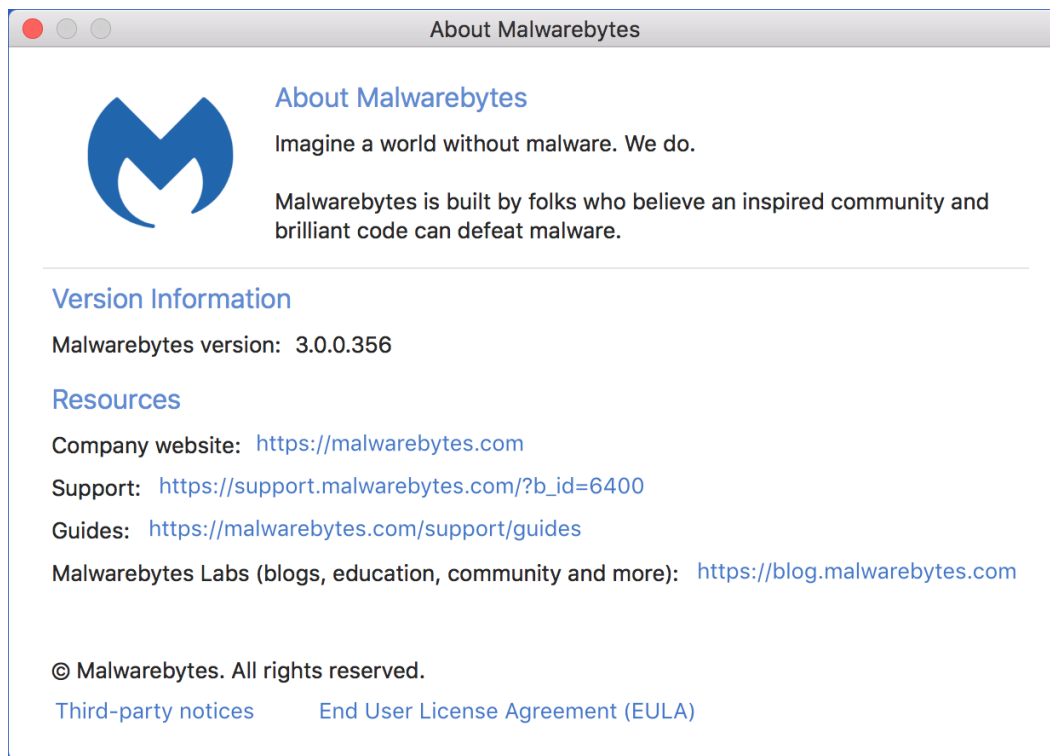
The upper panel contains <u>Version Information</u>. The <u>Resources</u> section provides contact addresses (URLs) which may offer assistance for sales, support, and educational purposes. In addition, you can view the third-party notices (open source software which we use in our products) as well as 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.
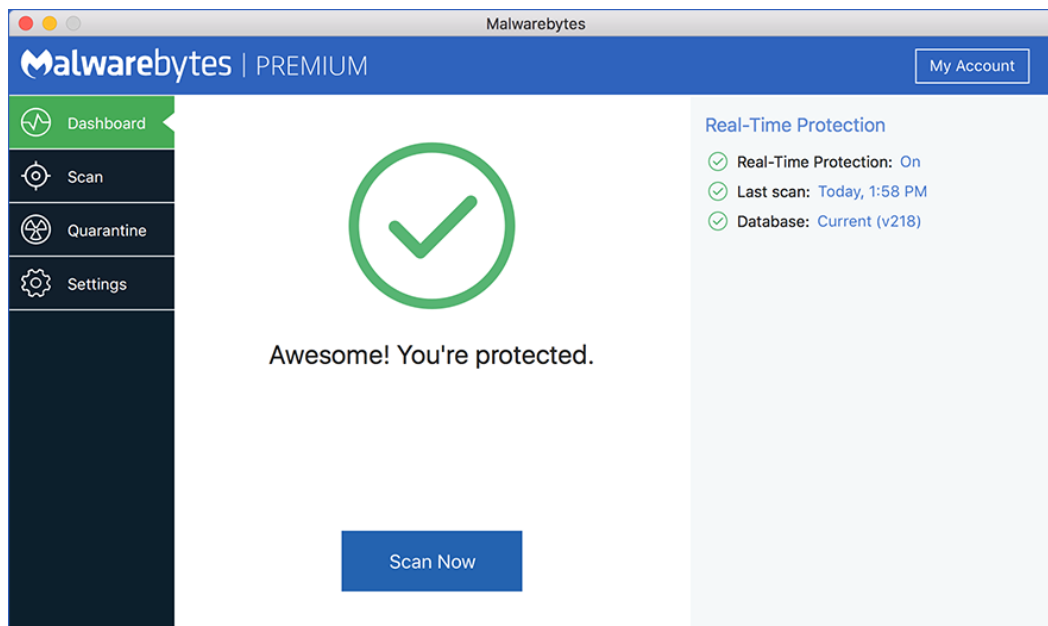
Status Pane

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:

Critical: Immediate attention is required.	**Warning:** Please take action before the situation becomes critical.	**OK:** 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.
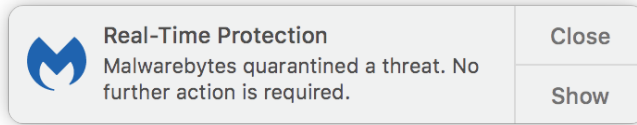
If you click **Close**, the notification will be dismissed. Clicking **Show** will launch the *Quarantine* screen, as shown on page 11.
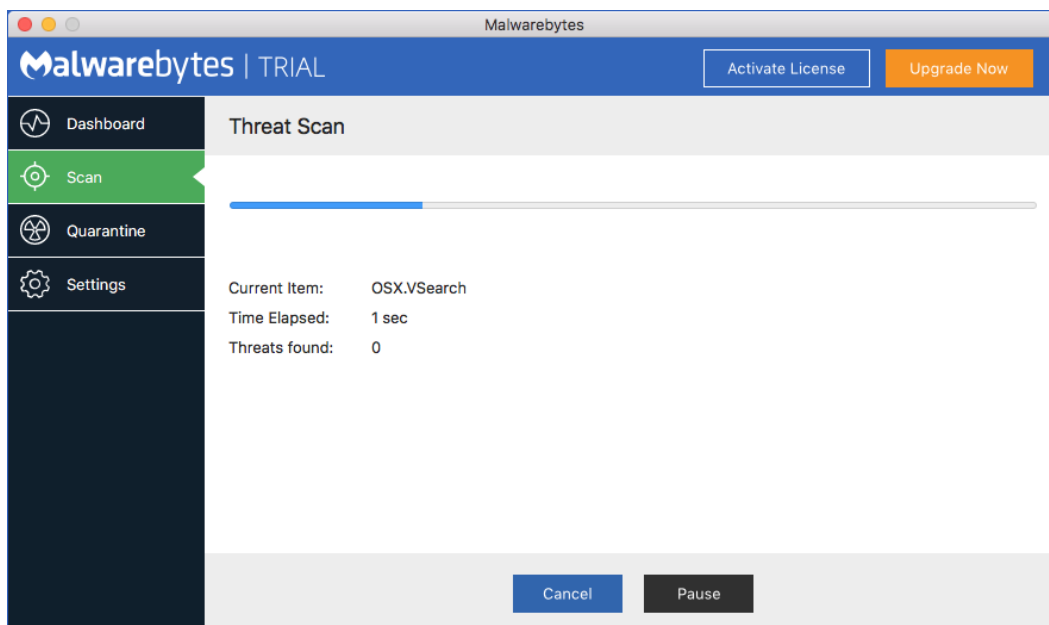
Scan

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.
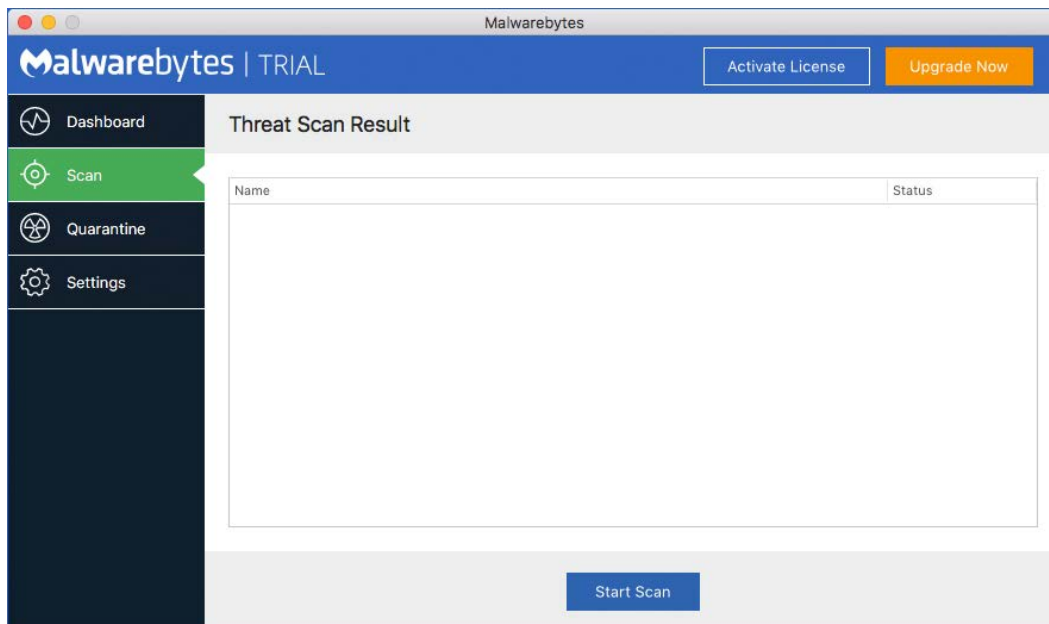
Click Start Scan to initiate a scan.

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.
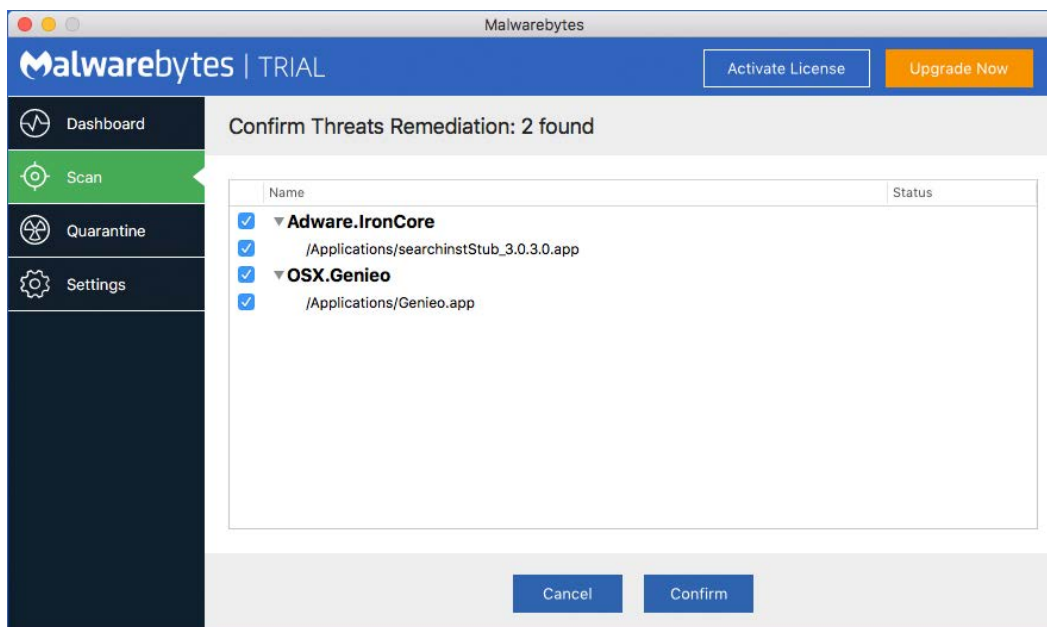
You may note that the screen shown here says that two threats were found, while it appears that four items are shown. The items shown in bold are the names of the threats themselves, while the information immediately below the threat name is a component of the threat. Threats may have several components. 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.
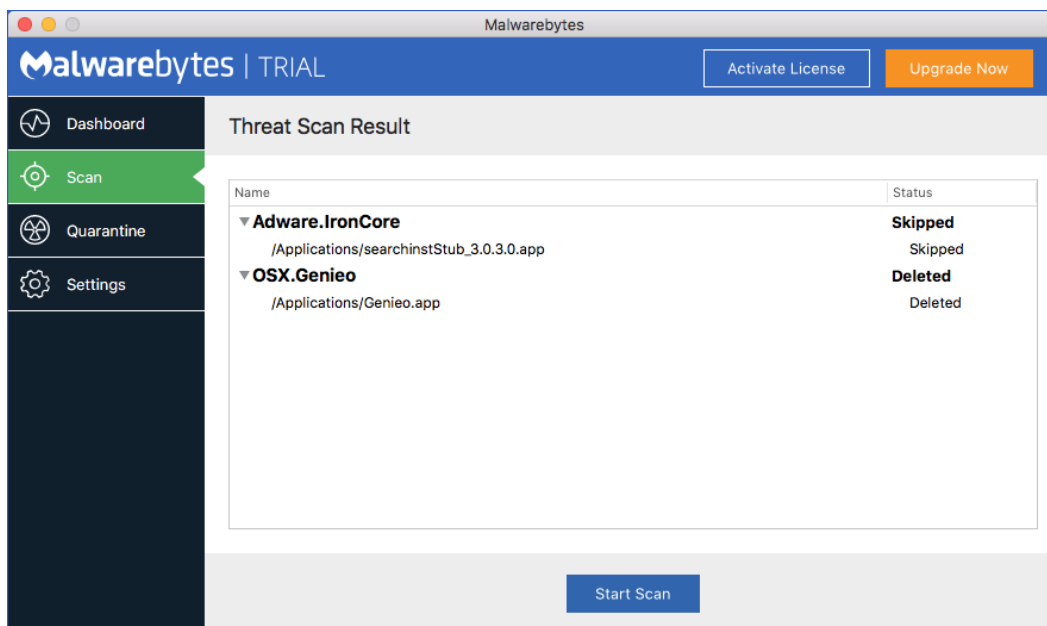
Threats which have been moved into Quarantine cannot harm your computer. They are neutralized as part of the Quarantine process, and can be processed further at any time.

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 <u>Show Quarantine</u> on the Quarantine screen. A screenshot is shown here.
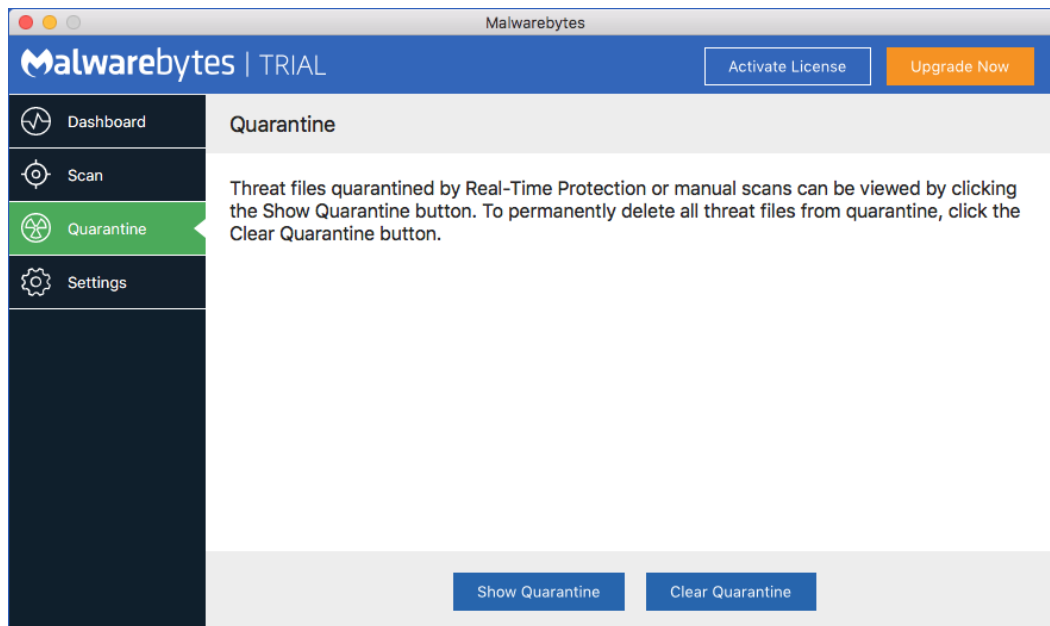

That will open a new system window showing the contents of the Quarantine folder. That system window is only there for your inspection. If you wish to delete the contents of the Quarantine folder, you should click <u>Clear Quarantine</u> in the *Malwarebytes* Quarantine screen. You will be presented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

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 two sections. Click on Settings in the menu panel to access settings. You will see the screen shown here.
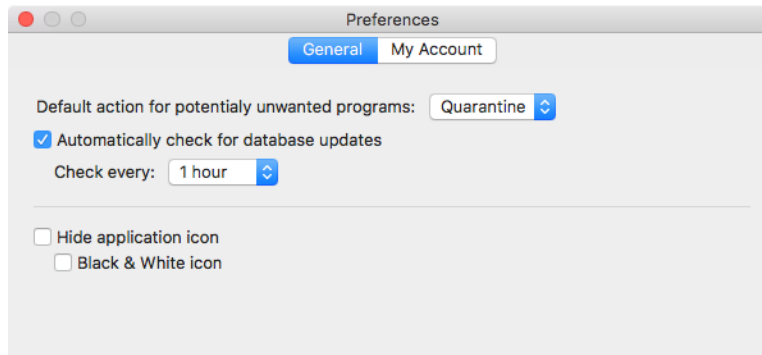
You will note that General is highlighted in blue, indicating it is the selected settings group. Available settings are:

- **Default action for potentially unwanted programs** 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 database 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** will cause the application 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).

The *My Account* tab has two variations. The first variation is for Free or Trial users. It offers the opportunity for the user to purchase a license, or to enter a license which they have already purchased. The screen is shown here.
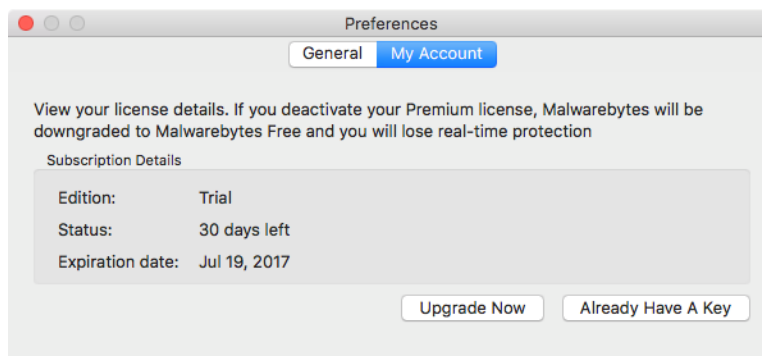
If they are using the Premium version of *Malwarebytes*, a slightly different screen is shown. This version takes into account that they have already purchased a license, and the two buttons at the bottom are replaced with the Change License Key button.