Malwarebytes for Mac v4
Product Guide

Malwarebytes™

2026

Table of Contents

Get Started

System requirements

This article lists the requirements for Malwarebytes Security version 4 on macOS devices.

System requirements:

- macOS:
- Sierra 10.12
- High Sierra 10.13
- Mojave 10.14
- Catalina 10.15
- Big Sur 11
- Monterey 12
- Ventura 13
- Sonoma 14
- An active internet connection.

Install Malwarebytes for Mac v4

Download and install the latest version of Malwarebytes for Mac version 4 to start removing threats from your Mac device. This article guides you through the installation process.

1. Double-click the file **Malwarebytes-Mac-4.x.y.zzz.pkg** to start the setup wizard. In most cases, downloaded files are saved in the Downloads folder.
   - **Note:** If you receive a security warning dialog, refer to Apple's article Open an app from an unidentified developer.
2. In the Install Malwarebytes for Mac pop-up window, click **Continue**.
3. Read the improvements and issues fixed in the latest version of Malwarebytes and click **Continue**.
4. Read the Malwarebytes Software License Agreement and click **Continue**.
5. Confirm you agree to the Software License Agreement, click **Agree**.
6. Confirm the installation Destination and Type, click **Install**.
7. In the pop-up window, enter your Mac User Name and Password and click **Install Software**.
   - **Note:** On macOS Ventura 13, click OK when prompted to allow access to your Downloads folder.
8. After Malwarebytes for Mac has finished installing, click **Close** to exit the setup wizard. Select **Keep** or **Move to Bin.**
9. When Malwarebytes initially opens, you see a welcome screen. Click **Get started** to continue.
10. Choose one of the provided options:
    - **Personal Computer:** a device owned by you or your family for home and personal use.
    - **Work Computer:** a device owned by your company or place of employment, like Malwarebytes for Teams customers.
11. Next, the Premium screen allows you to choose one of the following:
    - **Buy Now**: Click this button to view purchase options for a Malwarebytes subscription.
    - **Activate license:** Click this button if you already have a subscription. A new screen will appear where you can

sign in to My Account or enter a license key to enable your Malwarebytes subscription. For activation instructions, see Activate your subscription in Malwarebytes for Mac.
    - **Maybe later:** Click this button if you want to use the Malwarebytes Free edition. Certain features are unavailable in the Free edition, such as Scheduled Scans and Real-Time Protection. If a Trial is available, a screen appears with the option to start a 14-day Trial. Input your email to receive product and marketing emails, you can manage your communication preferences in your Malwarebytes Account. Click **Get started** to start a Trial.
- After a subscription is activated or a Trial is started, Malwarebytes for Mac requires permissions to enable Real-Time Protection:

On macOS Catalina 10.15 to Sonoma 14, you must give full disk access to Malwarebytes to enable Real-Time Protection and allow Malwarebytes to scan your Mac for threats. For detailed instructions, see Give Full Disk Access for Malwarebytes on Mac.

On older devices running macOS Mojave 10.14 or earlier, during the installation process, you're required to give Malwarebytes permission to enable Real-Time Protection on your Mac.

1. After the Premium screen option is selected, you are prompted to give Malwarebytes permission to enable Real-Time Protection on your Mac. Click **Allow**.
2. In the System Extension Blocked pop-up window, click **Open Security Preferences**.
3. Click the **Allow** button to enable Real-Time Protection.
4. Malwarebytes for Mac is now installed on your computer.

Activate Premium Features

Your Malwarebytes subscription allows you to activate paid features such as Real-Time Protection and Scheduled Scans. If you purchased a subscription for multiple devices, find instructions on how to install and activate on different devices here: Install and activate Malwarebytes personal products.

Activate using My Account

This method requires you to have an active Malwarebytes account login. If you haven't set up your My Account login, see Create your Malwarebytes Account.

1. Open the Malwarebytes application.
2. In the top right corner of the Dashboard, click **Activate License**.
3. In the Email field, enter the email address used to sign in to My Account.
4. In the Password field, enter the password used to sign in to My Account.
5. Click **Sign in**. When your subscription activates, click **Done**.

Activate using a license key

This method requires you to have your license key, see Find my Malwarebytes license key.

1. Open the Malwarebytes application.
2. In the top right corner of the Dashboard, click **Activate License**.
3. Click **Enter license key**.
4. Enter your license key into the License key field, then click **Activate license**.
    - **Note:** The Activate license button becomes clickable when a valid license key is entered into the corresponding

field.

5. Malwarebytes may ask you to allow or enable Real-Time Protection features. Click the **Turn Protection On** button that appears on the Dashboard.

When the Premium features are activated, Premium displays in the top-left corner of the program Dashboard.

Firewall Access Requirements

If you use a firewall and have Malwarebytes for Mac version 4 installed, your firewall application may block the connection to Malwarebytes update servers. This prevents you from activating your subscription or downloading protection and database updates.

To allow our app to connect to the Malwarebytes update servers, update your firewall to allow the following Web addresses and Malwarebytes processes.

Web Address	Port Number	Network traffic direction
https://data.service.malwarebytes.com	443	outbound
https://data-cdn.mbamupdates.com	443	outbound
https://*.mwbsys.com	443	outbound

Malwarebytes process	Internal file name
Malwarebytes	/Applications/Malwarebytes
Malwarebytes	FrontendApplication
Malwarebytes Agent	FrontendAgent
Malwarebytes Protection	RTProtectionDaemon
SettingsDaemon	SettingsDaemon

Give Full Disk Access

Malwarebytes for Mac version 4 requires Full Disk Access to detect threats found on your Mac. The app examines files to determine if they are malicious, it does not store or download these files. To enable Real-Time Protection and allow Malwarebytes to scan for threats, you must manually allow Full Disk Access permission to Malwarebytes Protection on your device.

The following macOS versions require you to provide Malwarebytes with Full Disk Access:

- macOS Catalina 10.15
- macOS Big Sur 11
- macOS Monterey 12
- macOS Ventura 13
- macOS Sonoma 14

To provide Full Disk Access on macOS Catalina, Big Sur, and Monterey devices, follow the instructions below, or click Learn how under the Malwarebytes needs more access notice for a guided tutorial.

1. On your Mac device, open **System Preferences**.
2. Click the **Security & Privacy** icon.
3. Click the **Privacy** tab.
4. Find Full Disk Access and select it.
5. Click the lock icon at the bottom-left corner of the windows to make Privacy changes.
6. You are prompted to enter your system Password to allow changes to your Security & Privacy. Enter your password and click **Unlock**.
7. Check the box next to Malwarebytes Protection in the list.
    - **Note:** If you do not see Malwarebytes Protection in the list, reinstall Malwarebytes for Mac, then enable Full Disk Access. You do not need to uninstall Malwarebytes first.
8. Once completed, click the lock icon at the bottom-left corner to prevent further changes to your settings.
9. You have granted Full Disk Access to Malwarebytes and can now close the System Preferences window.

To provide Full Disk Access on macOS Ventura and Sonoma devices, follow the instructions below:

1. On your Mac device, open **System Settings**.
2. Scroll, locate, and click **Privacy & Security**.
3. Under Privacy, click **Full Disk Access**.
4. Toggle Malwarebytes Protection **On**.
    - **Note:** If you do not see Malwarebytes Protection in the list, reinstall Malwarebytes for Mac, then enable Full Disk Access. You do not need to uninstall Malwarebytes first.
5. You are prompted to enter your login Password to allow changes to Privacy & Security. Enter your password and click **Modify Settings**.
6. You have granted Full Disk Access to Malwarebytes and can now close the System Settings window.

Edit Settings

Settings - General

The General settings is a tab on the Settings screen in Malwarebytes for Mac version 4. This section allows you to configure how Malwarebytes interacts with your Mac device. To view this screen, click the **Settings** cog icon in the top-right corner of the Dashboard, then click the **General** tab.

General is the default tab when you open Settings. Here you can configure a number of different operations for the program. Available settings are:

- **Default action for PUPs:** Determines the action taken on Potentially Unwanted Programs (PUPs). The default option is to Quarantine PUPs, but you may choose to Skip processing instead. This would exclude PUPs from scans, but you can still quarantine them by selecting them after a manual scan.
- **Automatically remove old items from Quarantine:** Malwarebytes neutralizes threats and puts them into Quarantine until you either restore or delete them. Keep this box checked if you want Malwarebytes to automatically delete these quarantined items after a set amount of time. You can set the time to have Malwarebytes delete quarantined threats after 30, 90, 180, or 365 days.
- **Automatically update to a new version of Malwarebytes:** This allows the application to automatically download and install updates in the background as soon as they become available. This setting is checked by default.
- **Automatically check for protection updates:** We recommend you select this option to benefit from the most current database updates. When selected, the Check every drop-down menu allows updates to schedule for once an hour, or up to once per 24 hours.
- **Hide application icon:** This causes the Malwarebytes application icon in the menu not to display. This settings is unchecked by default.
- **Black & White icon:** This causes the Malwarebytes application icon in the menu bar to display in monochrome when selected, or in color when not selected.
- **Beta Application Updates:** This causes Malwarebytes to download pre-release updates in addition to normal releases. This setting is unchecked by default.
- **Usage and Threat Statistics:** Switch the toggle to enable the application to send anonymized data to the Malwarebytes research team. This data helps our engineers improve the product and help protect you. For more information, see the Malwarebytes Privacy Policy.

Settings - My Account

The My Account tab in Malwarebytes for Mac version 4 allows you to view license key details, version status, and license key expiration date. You can also deactivate or change your license key on this screen. This is useful if you want to transfer a Malwarebytes Premium subscription to a different device. To view this screen, click the gear icon in the top-right corner of the Dashboard, then click the My Account tab.

The My Account tab in Settings looks different depending if you are using Malwarebytes Free, Malwarebytes Trial, and Malwarebytes Premium. Each version is described below:

- **If using the Malwarebytes Free version:** Real-Time Protection does not work. You can click I already Have A License to activate a Malwarebytes subscription, or you can click Upgrade Now to purchase a Malwarebytes subscription.
- **If using the Malwarebytes Trial version:** This screen allows the option to activate a subscription, purchase a subscription, or deactivate your Trial. If you deactivate your Trial, Real-Time Protection deactivates and you cannot resume your Trial.
- **If using the Malwarebytes Premium version:** This screen displays your license key. You can use the bottom buttons to Change License Key or Deactivate License.

Settings - CPU Usage

You can control the maximum amount of processing power Malwarebytes uses during a manual or scheduled system scan.

Go to **Settings > Advanced > CPU usage**, where you can set the CPU usage to:

- **High (Recommended)** - Uses up to 100% of a single CPU core for faster scans.
- **Medium** - Uses approximately 50% of a single CPU core for a slower scan.
- **Low** - Uses approximately 25% of a single CPU core for the slowest scan.

Manage Malwarebytes

Menu Bar Access

You can access Malwarebytes for Mac version 4 from two different points on the menu bar for Mac. This article provides an overview of the Malwarebytes menu items on Mac device.

Malwarebytes menu

The Malwarebytes menu is visible in the menu bar at all times and represented by the Malwarebytes icon. Click on it to display a drop-down menu.

See the following for a description of each menu item:

- **Last Protection Update Check:** displays when the last check for database updates occurred. This item is not clickable.
- **Start Scan:** initiates a Threat Scan.
- **Stop Malware Protection:** disables real-time protection against malware on the hard drive. When stopped, this option changes to Start Malware Protection.
- **Stop App Block:** disables the App Block protection feature. When stopped, this option changes to Start App Block.
- **Settings:** launches the Settings screen for Malwarebytes.
- **Update Protection:** checks the Malwarebytes servers for any available database updates.
- **Open Malwarebytes:** launches the Malwarebytes app.

Malwarebytes application menu

The Malwarebytes application menu is only visible when the Malwarebytes app is open and in the front of other apps on your Mac screen. Click Malwarebytes from the application menu to display a drop-down menu..

See the following for a description of each menu item:

- **About Malwarebytes**: shows the About screen for Malwarebytes. You can check your Malwarebytes version and other company information on this screen.
- **Check For Updates**: checks in with Malwarebytes servers for any version updates.
- **Preferences:** displays the Settings screen.
- **Services:** allows use of the 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:** displays content which had been hidden by Hide Others.
- **Quit Malwarebytes:** closes the Malwarebytes interface, while real-time protection remains active.

Find Version Number

This article gives you the steps to locate your Malwarebytes version number in your Mac device.

1. Open Malwarebytes for Mac.
2. In the top-left part of your screen, click **Malwarebytes** > **About Malwarebytes**.
3. In the About Malwarebytes pop-up window, your version number displays under Version information.

If you want to ensure your Malwarebytes app is up to date, visit Update to the latest version of Malwarebytes for Mac for details.

Change your License Key

To change your license key in Malwarebytes for Mac version 4 follow the instructions below.

1. Open Malwarebytes for Mac.
2. Click the **Settings** icon in the top right corner of the program window.
3. In the Settings pop-up window, click the **My Account** tab.
4. Click **Change License Key**. The pop-up windows offers the options to **Sign in** or **Enter license key** to activate your subscription.
5. Click **Enter license key**. This opens the Activate license window.
6. Enter your license key into the field. Be sure to include hyphens and capitalization.
7. Click **Activate**.

Security Advisor

Malwarebytes Security Advisor provides a comprehensive overview of your device's security and protection status and recommends ways to secure your device.

To use Malwarebytes Security Advisor:

1. Open Malwarebytes for Mac application from your desktop.
2. Locate and click the Shield icon on the top right corner of the app.
   Tip: The shield icon displays a red dot if there are unresolved issues.
3. The Security Advisor screen displays the recommendations based on your current settings. Click the button next to the recommendation to turn on that particular feature:
   - **Real-Time protection:** If any of the Real-Time Protection features are turned off, the Turn on button displays next to that particular feature. Click the button to turn on the applicable protection.
   - **Software updates:** This section notifies you of any pending software updates for the Malwarebytes app. Click Turn on to enable automatic updates for Malwarebytes.
   - **Device scans:** This section displays information regarding device scans, and notifies you if you haven't completed a scan recently and if you don't have future scans scheduled. Click Scan now or Schedule a Scan depending on which options apply.

Uninstall Malwarebytes for Mac v4

To uninstall Malwarebytes for Mac version 4, simply uninstall the program through Mac's Help menu.

1. Open Malwarebytes for Mac. If you have multiple apps open, make sure Malwarebytes is the one selected.
2. At the top of your Mac screen, click **Help**, then click **Uninstall Malwarebytes**.
3. A prompt appears with the following message: "This will completely remove the Malwarebytes software. Are you sure you wish to proceed?"
4. Click **Yes**.
5. Enter your Mac's password.
6. Click **OK**.

If you are unable to open Malwarebytes or access the Help menu, see Unable to reinstall Desktop Security on macOS device.

Run and Schedule Scans

Scan your device

Scanning your computer helps detect and remove malware, viruses, trojans, and other potentially unwanted items. If you have Malwarebytes on a Mac device, we recommend scanning your computer at least once a week, even if you have Real-Time Protection turned On.

Note: Malwarebytes for Mac v4 can not scan individual folders or external hard drives.

Run a scan

With Malwarebytes for Mac version 4, you can run a Threat Scan whenever your computer is turned on. Scheduled scans are available for the Malwarebytes for Mac Premium and Trial versions. After a scan finishes, you have the option to view a detailed scan report.

1. Open Malwarebytes for Mac.
2. On the Scanner card, click the blue **Scan** button.
3. If no threats were found, congratulations! If threats were detected, check the boxes next to items you want to quarantine.
4. Click **Quarantine** when finished selecting items.
5. After quarantining threats, the Scan summary displays. Here you can click:
   - **Done:** This button closes the Scanner card, bringing you back to the program Dashboard.
   - **Reports:** This tab shows rows of all previous scan reports. Click one to expand the details.
   - **View report:** This button shows expanded report details of the scan that that just finished. See below for an example scan report.
6. Click one of the Threats to see items that were quarantined of that type. You can scroll to the right to see a fourth column showing the full path. Hover your cursor over a path to reveal the entire file path.

Schedule a Scan

To create a scheduled scan in Malwarebytes for Mac version 4, you must have purchased a Premium subscription and activated the subscription in the application.

Create or edit a scheduled scan

1. Open Malwarebytes for Mac.
2. At the top-right of the program, click the **Settings** cog icon.
3. At the top of the Settings window, click **Scheduled Scans**.
4. The Default Scan displays. You can modify the default settings or create a new schedule scan.
5. If the scheduled scan is set to run and your computer is off or in sleep mode, the scan runs when the computer is powered on or awakened from sleep.
6. To add a new scheduled scan, click on the **+** icon. The New Scheduled Scan displays in the left pane.
7. Add the following information to configure the New Scheduled Scan:
   - Click in the **Name** field and rename the scan if you choose.
   - Check the **Allow this scan to be performed** checkbox.

- **Choose the Starts at**: date and time for the scan to run.
- Click the **How often** drop down menu to set the frequency for the scheduled scan.
- Check the **Quarantine malware automatically** checkbox.
- Click **Apply** to save changes.

8. **Note**: Malwarebytes Free version has no Scheduled Scans available. You must activate Premium on your Mac device to use this feature. Refer to "Activate Premium subscription."

Why Malwarebytes scans so fast on Mac devices

We are often asked why Malwarebytes on Mac scans the device faster than a Windows device. The reason is that Malwarebytes performs what's called a "quick scan." Rather than scanning the entire hard drive for files that are known to only be installed in specific locations, the scanner targets only items in those specific locations.

For example, when scanning for browser extensions, the scanner examines specific locations, outside of which a browser extension cannot function. Safari extensions can only install in Safari's extension folder (on older systems) or inside apps in the Applications folder on newer systems. Using this method, we not only keep Malwarebytes for Mac clean, lean, and fast, but we also limit the possibilities for false positives.

Additionally, starting with version 4.10 of Malwarebytes for Mac, we made significant caching improvements to avoid scanning files that have not changed since the last time they were examined. This means that there may be scans that happen even faster, and examine only a small number of files.

Manage Threats

Real-Time Protection

Premium subscribers of Malwarebytes for Mac version 4 gain access to Malware protection and App block which stops malicious files from executing on your device. Both of these features protect your system in advance, before malicious files can cause damage. The Real-Time Protection card is located at the lower-right side of the program Dashboard.

Protection layers

The Real-Time Protection card shows both protection layers that you can click to turn the features On or Off. If either of these layers are Off, the Dashboard prompts you to enable Real-Time Protection, or to upgrade to Malwarebytes Premium to activate these features. We recommend keeping them on to remain fully protected by Malwarebytes. The protection layers are available to Malwarebytes Premium subscribers and Malwarebytes Trial users. If the program reverts to the Free version, Premium dependent features will disable.

Both protection layers are described here:

Malware Protection

This feature protects your computer against malware, as well as adware and PUPs, by monitoring the hard drive. If malicious or unwanted files are created or modified, Malwarebytes identifies and quarantines them by default. This is similar to running a scheduled scan, except that the files are caught immediately, rather than at some undefined time later.

When malware protection detects a threat, a notification appears. No further action is needed at this point, other than optionally clearing the quarantine in Malwarebytes.

App Block

App Block aims to completely block applications from known bad developers, preventing them from running at all. When an application is blocked, a notification appears providing the name of the application that was blocked. The advantage of App Block is that it can detect and block new apps from existing developers, even if they have not yet been seen by Malwarebytes researchers. We recommend you keep App Block enabled to remain protected.

Activity Log

Malwarebytes for Mac version 4 saves records of events that occur in the program. To view these list of activities, click the Detection History card, then click the Activity log tab.

The Activity log screen displays different kinds of records which you can sort with the bottom-left filter. These event kinds are:

- Scans
- Quarantine
- Licensing
- Configuration
- Updates
- Notifications
- Miscellaneous

You can click the Date and Time header to sort the order of events displayed in Activity log.

The check-boxes to the left of each entry allows you to delete events. The Delete button becomes active once you have checked one or more events. Over time, Malwarebytes for Mac automatically deletes older activities to make room for new events.

Exclude Detections

Malwarebytes for Mac version 4 may block items, including applications and files that are not inherently malicious. There may be occasions when Malwarebytes for Mac flags items as malicious, but you want to keep them on your device. Add the item to your Allow List to stop Malwarebytes for Mac from detecting an item you know and trust.

When you add a detected item to the Allow List, it is omitted from future scans and protection events.

Add items to the Allow List

1. Open Malwarebytes for Mac.
2. Click the **Detection History** card.
3. Click the **Allow List** tab.
4. To add an item to the Allow List, click **Add**.
5. Select the item from the Finder app that you want to add to the Allow List.
6. Click **Open**.

Remove items from the Allow List

You can remove the items that you've added to the Allow List:

1. Click the item you want to remove from the Allow List.
2. Click **Remove**. You can also click Remove all followed by a confirmation to remove all the items in the Allow List.

Add to Allow List when restoring from Quarantine

You can directly add items to the Allow List when you're restoring them from Quarantined items:

1. Open Malwarebytes for Mac.
2. Click the **Detection History** card.
3. Under Quarantined items, select the item you want to restore and click **Restore**.
4. In the popup that appears, click **Restore and allow** to add the item to the Allow List.

Restore and Delete Quarantined items

You can find items removed by Real-Time Protection, scheduled scans, or manual scans in the Quarantined items tab. This feature encrypts all files that have been quarantined, making it impossible for those items to run or be detected by other antivirus software. Threats quarantined can either be deleted permanently or restored to their original locations. Items restored may be detected again in future scans. The program Settings allows you to choose whether and when quarantined items should be automatically deleted.

Restore or delete quarantined items

1. Open Malwarebytes for Mac.
2. Click the **Detection History** card.
3. Click the **Quarantined items** tab.
4. Click the check boxes next to each listed item you want to restore or delete.
5. You can either **Restore or Delete** selected items:
6. If you want to restore selected items back to their original locations, click **Restore**. In the popup that appears, click **Restore and Allow** if you want to exclude the item from future detections. Click **Restore only** if you don't want to add to the Allow List.
7. If you want to permanently delete selected items from your Mac, click **Delete**.

Automatically remove old items from quarantine

By default, Malwarebytes for Mac automatically removes old items from Quarantine after 90 days. You can toggle this feature on or off, and set a time interval for deletion by clicking the Settings cog icon Cog_21x21.png, then General. Here you see the option to Automatically remove old items from Quarantine. You can choose between 30 days, 90 days, 180 days, and 365 days for Malwarebytes to delete old quarantined items.

Troubleshooting

Can’t connect to the internet after scan

Malwarebytes for Mac version 4 scans for malware or adware and removes them from your device. Depending on the software, when Malwarebytes for Mac removes malware or adware from your device, the items removed may cause your device to lose its internet connection.

How this issue affects you

Your device is unable to connect to the internet after a Malwarebytes for Mac scan detected and removed malware or adware from your device.

What caused this issue

The malware or adware altered your network settings for your internet connection. The purpose of this malware was to either steal your personal information or show you unwanted advertisements. When you ran a scan on your device to detect and remove the malware, it was successfully removed. However, the changes to your network settings caused your device to lose its connection to the internet.

How to resolve this issue

To restore the internet connection, restart your macOS device. After your device has restarted, you should be able to connect to the internet.

If you still can’t connect to the internet after restarting your computer, you will need to manually fix your network settings. For instructions on how to access and change network settings from your device, see this Apple help article Change proxy settings on Mac or contact Apple Support.

Fix after effects of adware on Mac device

Malwarebytes for Mac scans and remediates threats found on your Mac device, but some kinds of malware can make changes to the Mac system that Malwarebytes cannot fix. These changes include:

- Malicious changes to the browser settings, such as your home page or search engine.
- Addition of malicious system profiles.
- Loss of internet connection after malware removal.

These changes may result in your browser continuing to redirect you to malicious sites, even after the malware has been removed. Malwarebytes can remove the malware responsible, but it cannot fix these changes to the Mac system.

To fix the issues described in this article, refer to the following resources:

- How to remove the after-effects of adware
- “Remove unwanted profiles on Mac device”
- “Can’t connect to the internet after scan”

Internet Browser Issues on Mac Devices

Malwarebytes products provide a safer, faster and more secure browsing experience, but they do not fix issues with your browser. Below are some common browser issues that may impact your browsing experience, and tips on how secure your online activity.

Common browser issues

Browser is slow or unresponsive

If your browser is slow to load a website, unresponsive or shows an error message, see these Apple articles:

- If Safari is slow, stops responding, quits unexpectedly, or has other issues
- If Safari doesn't load a page or webpage items are missing

Browser appearance changed

If you see an unfamiliar website, search box, or advertisement when you open your browser, it's possible something you downloaded or installed caused those changes. Browser preferences can be restored to their default settings, which may resolve changed setting issues.

Note: Resetting your browser settings may impact the way you usually use your browser. Review the instructions carefully to understand what settings of your browser are affected.

Receiving unwanted ads

If pop-up advertisements are appearing in your browser, consider blocking advertisements directly from your browser.

To help prevent unwanted pop-ups, refer to the Apple article: How to block pop-ups in Safari.

Browser notifications

You can allow certain websites to send notifications to your computer. These notifications may resemble advertisements and appear in the upper-right corner of your screen, even if your browser is closed. If you are seeing advertisements, it's possible notifications were enabled for a specific website.

If you want to stop seeing notifications from a specific website, refer to Apple's article: Customize website notifications in Safari on Mac.

For a safer and faster browsing experience, install Malwarebytes Browser Guard.

Secure online activity

Connecting to a site securely

Web addresses indicate if data transferred between a web browser and a website is done securely. Hypertext transfer protocol secure (HTTPS) is the secure version of HTTP (the protocol used to transfer data). HTTPS is encrypted, increasing the security of data transfer, which is very important when sensitive data is being accessed or sent, like when logging in to your email inbox, or your web banking site.

All websites should use HTTPS, particularly the ones that require a login.

In addition to the web address protocol, browsers include an icon that shows the site's security status. When secure, the information sent and received will be encrypted and can't be intercepted by bad actors, but it doesn't tell you about the site's reputation. Find out more about connecting securely to websites below:

- If you see a “Not Secure” warning while browsing the web with Safari
- Avoid fraud by using encrypted websites in Safari on Mac

Internet connection is not secure

When using a public internet connection, like in a coffee shop or library, it is usually not a secure network, because it is available to everyone. If a network isn’t secure, and you log into an unsecured site, other users on the network may see what information you access, send and receive.

If using a public internet connection, here are some things you can do to keep your information secure:

- **Connect to websites securely:** We tell you how to check if the connection to a website is secure in the previous section.
- **Use mobile data:** Using mobile data, which is usually encrypted, and isn’t shared with other users, is a safer option than a public connection.
- **Use a VPN app:** VPNs encrypt your online activity and make it look like your Internet traffic is coming from a VPN server rather than your own IP address. By using a VPN, people can’t find out who you are, where you are, or what you’re looking at.

To protect your online privacy and secure your WiFi connection, install our VPN.

If you have similar issues on multiple devices

If you’re having any of the issues above in more than one of your devices, it’s possible your network is compromised. To troubleshoot issues with your network, contact your Internet Service Provider (ISP) for assistance.

If the articles above did not help, refer to Apple Support to search for your inquiry.

Leftover Malwarebytes for Mac v4 file in StagedExtensions folder

On macOS, you may notice a file located at one of the following file paths:

- `/Library/StagedExtensions/com.malwarebytes.mbam.rtprotection.kext`
- `/Library/StagedExtensions/Library/Application Support/Malwarebytes/MBAM/Kext/MB_MBAM_Protection.kext`

The file above is not removed from your macOS after uninstalling Malwarebytes for Mac version 4.

Cause

macOS copies files into the StagedExtensions folder. The macOS technology System Integrity Protection (SIP) protects the StagedExtensions folder and its contents from being modified or deleted. Malwarebytes for Mac does not have permission to delete files that are located in the StagedExtensions folder.

If you try to delete files in the StagedExtensions folder, an error message appears.

For more information about System Integrity Protection, refer to Apple’s article About System Integrity Protection on your Mac.

Workaround

Should you feel it is necessary to delete files in the StagedExtensions folder, you can temporarily disable System Integrity Protection. Malwarebytes does not recommend or instruct users to disable Security Integrity Protection. Disabling System Integrity Protection may be dangerous and leaving this feature disabled is a potential security risk.

It is not necessary to remove the leftover file and we recommend you leave it in the StagedExtensions folder. The left-over file is not active and occupies a small amount of disk space.

Legacy System Extension Warning

In macOS 10.15.4 through 10.15.6, a warning message notifies you that kernel extensions will no longer be supported in future Apple updates.

If you are running Malwarebytes for Mac version 4.5.14 you will no longer see this message. All you need to do is update to the latest version of Malwarebytes for Mac, and verify automatic updates are turned on.

- To update, see our Update to the latest version of Malwarebytes for Mac article.
- To verify automatic updates are turned on, see "Settings - General."

For more information, see Apple's About Legacy system extensions article.

Troubleshoot Malwarebytes and macOS Mojave's TCC

There are some issues with Malwarebytes for Mac version 4 and macOS Mojave (10.14), due to a Mac feature called TCC. This article explains TCC, what the issues are, and how to work around them.

TCC Meaning

TCC is a Mojave feature that controls access to certain user data and stands for Transparency, Consent, and Control. TCC prevents apps from gaining access to things like contact info, e-mail messages, calendar data, etc, without explicit consent from the user.

How TCC conflicts with Malwarebytes

There are only two cases where TCC becomes a problem:

- **Minor problem** - Due to attempts to scan protected locations, a number of errors to show up in the system logs, primarily visible through the Console app. This is not actually an issue, and these can be ignored.
- **Significant problem** - Safari's Extensions folder is one of the TCC protected locations. Malwarebytes should not be able to scan this location by default, but there have been a few cases where it can, but then any attempt to quarantine a detected Safari extension may receive a Remedy failed error in Malwarebytes.

Removing these extensions doesn't matter. Apple only allows certain extensions to load in Mojave, and other extensions have to use a new mechanism that doesn't involve this protected folder. So, even if a bad extension is present, it can't be loaded.

Solution for Remedy failed error

Give access to Malwarebytes Protection by following these instructions:

1. Open **System Preferences > Security & Privacy > Privacy**
2. Select the **Full Disk Access** item in the list.
3. Click the lock in the bottom left corner of the window to unlock the preference pane.
4. Click the **+** button below the list of apps.
5. In the file selection dialog that opens, press **command-shift-G**.

6. Enter the following path, then press **Go**:
   `/Library/Application Support/Malwarebytes/MBAM/Engine.bundle/Contents/PlugIns/Malwarebytes Protection`
7. Select Malwarebytes Protection, then click **Open**.

Unable to Activate Real-Time Protection

At times, there can be technical issues when trying to activate Real-Time Protection with Malwarebytes for Mac version 4. On macOS 10.13 (High Sierra) or later, Apple requires your approval to allow the Real-Time Protection feature. For more information, see Real-Time Protection in Malwarebytes for Mac v4.

Malwarebytes may ask you to allow the Real-Time Protection feature at the system level. In your Mac's Security & Privacy settings, you should see an Allow button that you must click in order to grant Real-Time Protection access on your device. If you are running into issues where you cannot activate Malwarebytes' Real-Time Protection, try either troubleshooting tips below.

Allow button appears but doesn't respond

When the button appears but does not respond, you may be in one of these scenarios:

- You are sharing your screen.
- You are connected to a docking station.
- Your Mac has software installed like a tablet driver or a third-party mouse.

Disconnect all third-party devices and click the button using the Mac track pad or with an Apple mouse connected to your Mac.

If problems persist, you may need to disable third-party applications through safe mode. Try the following steps:

1. Restart your computer in safe mode. See How to use safe mode on your Mac under the section How to use safe mode.
2. Reinstall Malwarebytes for Mac.
3. Restart your computer normally.

Allow button doesn't appear or Activate Protection button doesn't respond

Damage to a system managed folder in your Mac can cause issues when turning on Real-Time Protection. You may encounter a warning pop-up window.

If you encounter this issue, you can reinstall your MacOS. For instructions, see How to reinstall macOS from macOS Recovery. Try to activate Real-Time Protection again after installing the latest macOS.