Malwarebytes for Windows v4
Product Guide

Malwarebytes™

2026

Table of Contents

Get Started

Install Malwarebytes for Windows

Download and install the latest version of Malwarebytes for Windows version 4 to start protecting and removing threats from your computer.

1. In the Downloads folder, double-click the MBSetup.exe setup file.
    - Note: Downloaded files are usually saved to the Downloads folder. If you're unsure where your downloaded files are being saved, refer to Windows' article here.
2. If the User Account Control pop-up window appears, click Yes to allow the installation of Malwarebytes for Windows.
3. Click Install. To choose a different install location, click Advanced Options.
4. When asked Who are you trying to protect? choose one of the following:
    - Me or my family: Select this option if you're using the device in a home setting.
    - My organization: Select this option if you are using the device in a business environment.
5. The next screen asks you to install Malwarebytes Browser Guard for browser protection.
    - Click Yes, sounds good to install Browser Guard along with the antivirus and security app.
    - Click Skip this for now if you already have it installed, or want to find out more about this product before installing it. To learn more, see the Browser Guard product page.
6. The installation may require a restart. Save your work before clicking Restart computer.
    - Note: The installer will re-open once the computer restarts.
7. After the installation is complete, click Done.
8. Open the Malwarebytes app and click Get started.
9. Click one of the following buttons:
    - Buy now: Purchase a Malwarebytes subscription to unlock all protection features.
    - Activate Subscription: Sign in with your My Account credentials or enter your license key to activate your Malwarebytes subscription.
    - Maybe later: Activate a free 14-day Trial. If you've already used your Trial period, the Malwarebytes Free version opens instead, which only removes existing threats and has no proactive protection.
10. You are taken to the main Dashboard of the program.
    - Note: To pin Malwarebytes for Windows to your taskbar, click HERE for instructions.

To activate a Malwarebytes subscription after installation, see Activate your subscription in Malwarebytes for Windows.

System requirements

This article lists minimum system requirements for Malwarebytes for Windows version 4.

System requirements

- Operating System: Windows 11, Windows 10, Windows 8.1, Windows 8, or Windows 7 SP1
    - Note: For Windows 7 devices, you need to apply the Microsoft 2019-09 Security Update.
- CPU: Minimum 800 MHz 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. ARM-based Windows devices and Windows OS on Mac devices with Apple Silicon (M1 chip, ARM-based) processor are not supported.
- RAM: 2 GB (64-bit OS), 1 GB (32-bit OS).

- Free disk space: Minimum 1 GB.
- Recommended screen resolution: 1024x768.
- An active internet connection.

Activate Subscription

Your Malwarebytes for Windows version 4 subscription allows you to activate Premium 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.

There are two ways to activate your subscription.

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 Subscription.
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.
6. Once activated, Premium displays in the top-left corner of the program Dashboard.

Activate using a license key

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

If your license key has this format XXXXX-XXXXX-XXXXX-XXXXX, follow these steps:

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

If your license key has this format XXXX-XXXX-XXXX-XXXX and has a license ID with the format XXXXX or XXXXX-XXXXX, follow these steps:

7. Open the Malwarebytes application.
8. Click Activate Subscription from the top of the application window.

- In the Email field, enter the email address used to sign in to My Account.
- If you forgot your My Account email or password, click the Forgot password link.

9. If you have not yet registered your license key with My Account click the Sign up link and create a new account.
10. In the Password field, enter the password used to sign in to My Account.
11. Click Activate.
12. Once activated, an Activation successful notification is displayed in the product.

Malwarebytes for Windows as an Anti-Virus software replacement

Malwarebytes for Windows version 4 is a complete antivirus alternative. We use a comprehensive solution, with advanced technologies like anomaly detection, behavioral analysis, and application hardening to crush viruses and other types of malware. If you still wish to use other antivirus software, Malwarebytes works alongside and is compatible with most other security products available today.

See our Malwarebytes product page for more information on how Malwarebytes protects you from the most dangerous forms of malware.

Malwarebytes not only cleans up damage caused by malware, but most importantly, actively protects you before malware strikes. Features include:

- Malware Protection
- Web Protection
- Exploit Protection
- Ransomware Protection

There are alternate compatibility settings offered within Malwarebytes for users with an existing Anti-Virus on their PC. See Malwarebytes for Windows and Windows Action Center (WAC).

For more information on Malwarebytes for Windows:

- Frequently Asked Questions - Anti-Virus Replacement
- Malwarebytes 4.0 Blog announcement

Help icon

Malwarebytes for Windows version 4 offers a Help page to display different resources and troubleshooting content. To view this page, click the question mark icon 2020-08-07_8-05-30.jpg in the top-right of the header. Click one of the cards to access a self-help resource. At the bottom of the page, the Frequently asked questions section gives a list of articles to help for common issues..

Malwarebytes for Windows Trial

After you install Malwarebytes for Windows version 4 for the first time, a Malwarebytes Premium Trial is offered. With the Malwarebytes Premium Trial, you get to experience a comprehensive cyber security program that crushes established and emerging threats before they can disrupt your digital lifestyle.

Your 14-day Malwarebytes Premium Trial enables features that:

- Protects your identity and privacy from hackers
- Protects your documents, financial files from ransomware
- Protects you from malicious and fraudulent websites
- Stops malware that slows down your computer
- Crushes attacks that corrupt your programs

Malwarebytes Premium Trial offers the Play Mode feature, which hides Malwarebytes notifications on your computer during gaming, streaming, and presentations.

Edit Settings

Settings - About Tab

The About tab in the Settings section of Malwarebytes for Windows version 4 shows your program version information such as the Update package version and Component package version. To view your Settings, click the gear icon in the top-right corner of the Dashboard and click the **About** tab.

Under your Malwarebytes version number is a blue **Check for updates** button. Click this button to have Malwarebytes check our servers for the latest database, component package, and Malwarebytes version updates. Below the Check for updates button, the date of your last update displays.

At the bottom of the About screen are links to the Third party notifications and the End User License Agreement (EULA). Click these links to open either document in your web browser to learn more.

Change display language

To change the Malwarebytes for Windows version 4 language, you can do so from the **Settings General** tab. After the language is changed, the interface, notifications, and error messages are translated into the language you have selected.

How to change the language

1. Open Malwarebytes for Windows.
2. Click the **Settings** button, then select the **General** tab.
3. Scroll down to the Language section.
    - **Note:** The Language section is the third section down in the General tab.
4. Under Language, click the drop-down menu to choose your preferred language.
5. Supported languages: Bulgarian, Chinese (Traditional), Czech, Danish, Dutch, English, Finnish, French, German, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese (Brazil), Portuguese (Portugal), Romanian, Russian, Slovak, Slovenian, Spanish, Swedish.
6. Once you have chosen your preferred language, you may exit Malwarebytes for Windows.

Settings - Display tab

The Displays settings in Malwarebytes for Windows version 4 allows you to change your theme and background as well as toggle your hardware acceleration on or off.

How to change your app's theme

These steps guide you on how to change the theme of your Malwarebytes application.

1. In your Malwarebytes dashboard, click the gear icon to navigate to **Settings**.
2. Click the **Display** tab.
3. In the Theme section, click the radio button that corresponds with your background preference. You have the following options as a theme:
    - **Use system default:** Malwarebytes adopts the same light or dark theme as your Windows operating system. Users on operating systems earlier than Windows 10 will not see this option.

- **Light:** Malwarebytes displays using dark text and a lighter theme.
- **Dark:** Malwarebytes displays using light text and a darker theme.

How to change your app's background

These steps guide you on how to change the background of your Malwarebytes application.

1. In your Malwarebytes dashboard, click the gear icon to navigate to **Settings**.
2. Click the **Display** tab.
3. In the Background section, click the radio button that corresponds with your background preference. You have the following options as a background:
   - Cityscape
   - Data web

Toggle hardware acceleration settings

Turning on your hardware acceleration settings can increase your device's display performance. Turn off hardware acceleration if you encounter text display issues. By default, hardware acceleration is off.

1. In the Malwarebytes dashboard, click the gea icon to navigate to Settings.
2. Click the **Display tab**.
3. Scroll down to the **Hardware acceleration** toggle.
4. Click the **Hardware acceleration toggle** to turn hardware acceleration on.
5. In the pop-up window, click T**urn on and restart**. Malwarebytes restarts to apply the changes. You can click the toggle again to turn hardware acceleration off.

Enable Brute Force Protection

Cybercriminals may try to gain remote access to your devices by submitting many passwords in hopes of guessing one correctly. This is also known as a brute force attack. Our Brute Force Protection (BFP) feature monitors Microsoft's Remote Desktop Protocol by protecting your devices from suspicious connections via remote devices. It temporarily blocks IP addresses with suspicious login attempts and notifies you of the blocks. You can also customize the criteria for a brute force attack using the additional settings.

Note: BFP is an opt-in feature and is available only for Malwarebytes for Windows and Malwarebytes for Teams users. Ensure that you update the app to the latest version to avail this feature. See "System requirements" on page 2 to check if your device is compatible with the latest version.

How to enable BFP

To enable BFP:

1. Open Malwarebytes for Windows application from your desktop.
2. Click the Settings icon and select the **Security** tab.
3. Switch on the toggle under the **Brute Force Protection** section.

Note: Turning on this feature does not enable the Remote Desktop Protocol if you have not enabled it in your Windows settings.

Advanced Settings

Once Brute Force protection is enabled, you can further customize the criteria for blocking the suspicious IP address:

1. Click **Advanced** under Remote Desktop Protocol (RDP).
2. Click the **Edit** icon in the top right corner of the window that appears.
3. We recommend to retain the existing value in the **Port** field. However, you can change the value based on your protocol requirements. You can also click **Restore default** to go back to the default value.
4. Configure a **Trigger rule** depending on how many failed logins are attempted within a certain timeframe and how many minutes you want to block the IP address.
5. Click **Save**.

Note: BFP will not block devices connected to your private network.

Settings - General Tab

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

You can scroll through the General setting to see several configurable items. Read further for a description of each.

Application Updates

Malwarebytes periodically releases program updates for components or the full program. This setting offers two toggle switches for the program to automatically download and install component updates, and if you want to receive notifications when full version updates are available. Click **Check for updates** to check for database, component package, and Malwarebytes version updates.

Windows Explorer Settings

This setting allows the option to scan individual files and folders while in Windows Explorer. Right-click a file or folder to bring up the context menu and select **Scan with Malwarebytes**. This setting allows you to toggle this feature on or off. By default, this is set to **On**.

Language

This setting determines the language used throughout the program. This is pre-set, based on the language used during program installation. You can change it anytime by clicking the drop-down menu and selecting a language from the list.

Manual Scan Performance Impact

Malwarebytes manual scans may affect the performance of lower-powered computers. This setting allows you to choose whether manual scans have a higher or lower priority when multiple other tasks or programs are running. Lower scan priority requires more time to execute, but affects computer performance less. Higher scan priority allows manual scans to execute more quickly but may affect other tasks.

Event Log Data

This setting provides additional information regarding program actions beyond what is normally reported. If you encounter a technical issue with Malwarebytes, a Customer Support agent may request that you toggle on this setting to provide additional troubleshooting information. Once Malwarebytes Support receives these troubleshooting logs, turn this setting to **Off** to prevent impacts to device performance. By default, this is set to **Off**.

Tamper Protection (Premium only)

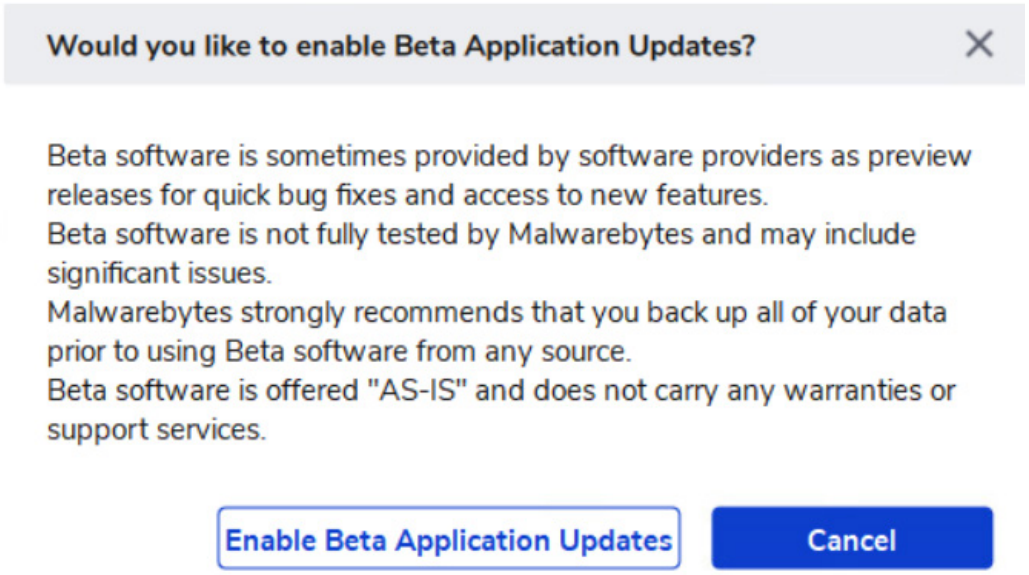
This setting allows Malwarebytes Premium and Malwarebytes Trial versions to restrict program features and functions with password protection. The **Manage Protection** button is only visible when this setting is toggled On, allowing the user to define program sections which require a password to access.

When you click the **Manage Protection** button, a pop-up window displays where you can restrict user access to certain areas of the program only to people who have the password. Click **Next**, and a window where you can set a password appears.

Note: If you forget your Tamper Protection password, it can be reset using your license key, or the key portion of your license, if your license is in the older ID and Key format. In the Tamper Protection window, click Reset password, then enter your license key (capitalized and including dashes) to set a new password.

Beta Updates (Premium only)

Toggle this setting On if you want to try the newest features as soon as they are available. When toggled on, you see the following window.



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.

For Malwarebytes for Teams customers, this toggle enables email reports and device alerts.

Proxy Settings

Use this setting if your internet connection utilizes a proxy server. This feature is usually used on a corporate network and has two primary purposes:

- Funnel communications to and from the outside world through a single connection point. This assures anonymity of all devices on a single network.
- Cache content to greatly converse bandwidth.

By default, this is set to **Off**. If toggled **On**, the setting menu changes to all you to configure proxy server details.

You can now specify the IP address or name of the proxy server in the **Address** field. Set the appropriate port number in the **Port** field. The person who controls access to the proxy server should know if proxy server authentication is required, and if so, toggle **On** the Proxy server authentication switch and provide a Username and Password assigned to your device.

The **Restore default settings** button at the bottom of General settings will reset all configurations on this screen as if you first installed the program.

Hide Notifications using Play Mode

Play Mode allows you to hide Malwarebytes for Windows version 4 notifications when selected apps are open on Windows devices. We recommend enabling Play Mode when playing games, watching movies, and giving presentations. This article explains how to enable and disable Play Mode, and how to select the applications that you want to use in Play Mode. Play Mode is available for Malwarebytes Premium subscribers.

Turn Play Mode On or Off

1. Open Malwarebytes for Windows.
2. Click **Settings**, then click the **Notifications** tab.
3. Scroll down to the Play Mode section.
4. **Suspend notifications and updates when selected apps are open** toggle is **On** by default. Switch off the toggle if you wish to always see Malwarebytes notifications.

You can add new applications to the Play Mode list to hide Malwarebytes notifications while using the app. Learn how to manage applications for the Play Mode feature below.

Manage Applications for Play Mode

1. Click **Add** in the bottom right of the Play Mode section.
2. Select the application and click **Open**. The application gets added to the Play Mode list.
3. To delete an application from the list, hover the cursor over the application name, and click the **Delete** icon that appears.

Settings - Notifications

Configure notifications settings related to scans, Real-Time Protection, updates, and subscription status in the Notifications tab of the Settings screen in Malwarebytes for Windows version 4. Malwarebytes Premium subscribers can pause notifications from displaying, using the Play Mode feature. Access notifications settings by clicking the Settings gear on the top-right corner of the Dashboard, then selecting the Notifications tab.

Notifications

Notification windows pop-up in the lower right corner of your screen, outside of the Malwarebytes interface, unless indicated otherwise.

- **Show a monthly security summary**: Available for paid and trial users. Enable this setting to receive a summary of detected threats via an in-app pop-up. By default, this toggle is enabled.
- **Show all notifications in Windows notification area:** Available for paid, trial, and free users. Enable or disable non-critical Malwarebytes notifications appearing in the Windows notification area. By default, this toggle is enabled.
- **Hide notifications when scheduled scans complete without threats detected:** Available for paid and trial users. Enable or disable notifications for completed scheduled scans that include no threats detected. By default, this toggle is disabled.
- **Alert me if any Real-Time Protection modules are turned off:** Available for paid and trial users. Enable this setting to receive notifications when a Real-Time Protection module is disabled. By default, this toggle is enabled.
- **Close non-critical notifications after:** Available for paid, trial, and free users. In the drop-down menu, set the duration for the notification display time, or choose to keep Malwarebytes notifications open until you manually close them.

Marketing Preferences

- **Show promotional notifications from Malwarebytes:** Available for paid, trial, and free users. Enable this setting to receive promotional notifications from Malwarebytes in the lower right corner of your screen, outside of the Malwarebytes interface. This setting does not impact promotional notifications displayed in the Malwarebytes app window, and is enabled by default for all users.

Scan Reminder

Available for paid, trial, and free users.

- **Get reminded to run a scan when new files or or programs are downloaded:** Enable this setting to receive a scan reminder after a new file or program is downloaded. This setting is enabled by default for free users. Once enabled, use the Notify me drop-down to select how often you want to be reminded. Options include Hourly, Daily, Weekly (recommended), and Every 2 weeks.
- **Get notified when a scan hasn't been run after a specified number of days:** Enable this setting to receive periodic notifications to run a scan with Malwarebytes. Once enabled, use the Notify me after drop-down to select how often you want to be reminded. Options include 1 day, 3 days, 7 days, 14 days, and 30 days.

Play Mode

Available for paid and trial users.

Enable Play Mode to hide Malwarebytes notifications when certain applications are in use. We recommend enabling

this feature during movies, gaming, and presentations. Add apps to Play mode to prevent notifications displaying when using them. If a notification occurs that requires user action, it is displayed after you close the apps that are added in Play Mode.

To add an application to Play Mode:

1. Click **Add**.
2. Enter the app's full path or file name into the **File name** field, or to navigate to the file location.
3. Click **Done**.

To remove apps added to Play Mode, click the trash bin icon next to the app entry.

Settings - Security

Configure how Malwarebytes protects your device in the Security tab of the Settings screen in Malwarebytes for Windows version 4. Access Security settings by clicking the Settings gear on the top-right corner of the Dashboard, then selecting the Security tab. Malwarebytes Premium subscribers and Trial users benefit from additional settings. Scroll through the Security settings to see all configurable items.

Update Threat Intelligence

Available for paid, trial, and free users.

Enable this setting to automatically check for protection updates, and set the interval when the checks occur, between every 15 minutes and 14 days. You can set the increment to minutes, hours, and days. This setting is On by default.

Automatic Quarantine

Available to paid and trial users.

Automatically quarantine malware upon detection

Specify if threats are automatically quarantined when detected. This setting is On by default. If the setting is toggled off, a notification displays in the lower right corner of the screen for each detection, and you must specify how to action the detection. Options include:

- **Ignore once:** the threat remains on the device, but will be detected in the next scan.
- **Ignore always:** the threat is added to Allow list and will not be detected again.
- **Quarantine:** the threat is removed and placed in quarantine, where it no longer impacts the device.

Automatically unquarantine when detected malware is a false positive

When Automatic quarantine is enabled, this setting allows Malwarebytes to automatically restore detections that were quarantined but were later found to be false-positive detections. When a detection is restored, a notification displays in the in-app notification center, and the event can be reviewed in detection History reports. This setting is On by default. If this setting is off, false-positive detections must be restored manually.

Windows Startup

Available to paid and trial users.

Define how Malwarebytes behaves when your computer starts. Your computer may launch several applications at start-up, initiating processes which need Malwarebytes launch timing to be adjusted. Keep this feature On for Malwarebytes

to launch in the background when Windows starts.

Descriptions for each Advanced setting are as follows:

- **Launch Malwarebytes in the background when Windows starts up:** Malwarebytes and Real-Time Protection layers start when Windows operating system starts. If disabled, Malwarebytes and Real-Time Protection layers do not start with Windows, but can be started manually by launching Malwarebytes.
- **Delay Real-Time Protection when Malwarebytes starts:** When the startup of system services used by Malwarebytes conflicts with services required by other applications at boot time, enable this setting, and adjust the delay timing. 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. Check this box to introduce a one-time delay as the self-protection module is enabled.
- **Enable self-protection module early start:** When enabled, the self-protection module starts earlier in the computer's boot process. This changes the order of services and drivers associated with your computer's startup.

Scan Options

Available to paid, trial, and free users.

Configure the Malwarebytes rules used for running manual scans on your devicely. For information about setting scheduled scans, see "Set up automatic scans in Malwarebytes for Windows".

- **Scan for rootkits:** A specific set of rules is used during scans to determine if rootkits are present on your device. Rootkits are malicious software that can modify operating system files and hide their presence. Toggling this setting on will make scans more intensive and effective, but increase the time to complete them. By default, this setting is Off.
- **Scan within archives:** When enabled, Malwarebytes scans two levels deep within archive zip, rar, 7z, cab and msi files. If disabled, archives are excluded from scans. By default, this setting is On.
- **Use artificial intelligence to detect threats (scans may take longer):** Toggling On to supplement existing detection methods by using machine learning to identify malicious files.
- **Use expert system algorithms to identify malicious files:** Toggle On to supplement existing detection methods by using expert system algorithms to identify malicious files. Available for paid and trial users.

Windows Security Center

Available to paid and trial users.

Malwarebytes Premium and Trial versions register as a security solution on your Windows device by default. If kept enabled, your Windows operating system recognizes Malwarebytes as your security solution. If you run any other anti-virus software, you may need to register that program with Windows Security Center separately.

Potentially unwanted items

Available to paid, trial, and free users.

Malwarebytes detects non-malicious software called Potentially Unwanted Programs (PUPs) and Potentially Unwanted Modifications (PUMs). PUPs appear in the form of toolbars and other software usually installed on your computer as part of a bundle. PUMs are usually related to the Windows registry. Configure how you want Malwarebytes to handle PUP and PUM detections during scans and Real-Time Protection events:

- **Detect Potentially Unwanted Programs (PUPs):** Use the drop down menu to select Ignore Detection, Warn User, or Always (recommended).
- **Detect Potentially Unwanted Modifications:** Use the drop down menu to select Ignore Detection, Warn User, or Always (recommended).

Brute Force Protection

Available to paid and trial users.

Brute Force Protection (BFP) monitors Microsoft's Remote Desktop Protocol, protecting your devices from suspicious connections via remote devices. It temporarily blocks IP addresses with suspicious login attempts and notifies you of the blocks. BFP is available only for Malwarebytes for Windows and Malwarebytes for Teams users. Learn how to "Enable Brute Force Protection" on page 10.

Exploit Protection

Available to paid and trial users.

Exploit Protection shields legitimate programs from potential vulnerability exploitation, by detecting and blocking attacks that go undetected by other security apps. This feature has the following options:

- **Block potentially malicious email attachments (Outlook desktop only):** Blocks malicious file attachments sent through your Outlook app.
- **Block penetration testing attacks:** Blocks exploits used by third-party tests.

Click Manage protected applications to review a list of your protected apps. Apps protected by Malwarebytes appear under the Default tab, while apps you manually add display under the Custom tab.

To add apps to Exploit Protection:

1. Click the **Custom** tab.
2. Click **Add**. This opens a new window.
3. Enter an app name in the **Application name** field.
4. Click **Browse** to select the app file you want to add.
5. Use the drop-down menu to select a **Program type**. If you are unsure of the type of program, select **Other**.
6. Click the blue **Add** button to save your entry.
7. The entry appears under the Custom tab where you can toggle protection on or off. Hover your cursor over the entry and click the pencil icon to edit, or click the trash icon to delete the entry.

Click **Advanced Settings** to view and configure additional details of Exploit Protection. Use the check boxes to enable or disable protections for specific protection layers, and the tabs to change views between different protection categories. We recommend only changing advanced settings when requested by a Malwarebytes Support representative. Incorrect settings may result in impaired protection.

Trusted Advisor

When it comes to device security, blocking and removing malware is just one of the many layers of protection you get with Malwarebytes for Windows version 4. While active protection and conducting routine scans are essential compo-

nents of device security, Trusted Advisor helps you keep track of many other factors that are important for security and critical factors in your privacy and device health.

Whether you're an avid techy well-versed in cybersecurity, or someone who is buying your first computer, Trusted Advisor makes security, protection, and privacy a breeze. Trusted Advisor combines the proven capabilities of Malwarebytes with the knowledge of the brightest industry experts to deliver an all-encompassing read out of your protection strength. Trusted Advisor comprises four main components to provide a holistic assessment of your security and privacy posture in a way that makes it easy to take action on items that negatively impact your protection.

Trusted Advisor components

- **Dashboard status:** An easy-to-read percentage score and rating provide an at-a-glance read-out to see if you are in good standing or if action is required to crush gaps in your protection. When we detect problems, you'll instantly know how many issues need your attention, and getting started is as easy as clicking the **See Recommendations** button.
- **Detailed overview page:** Here, you'll find a list of items requiring your attention, along with additional details on resolving issues. Advanced users will appreciate the ability to custom tailor the Trusted Advisor to their individual needs by specifying what gets monitored and what should be ignored.
- **Alert notifications:** When we spot an issue, Trusted Advisor keeps you well informed with optional desktop notifications that alert you when action is required.
- **Powerful and robust monitoring:** Trusted Advisor is like having your own personal team of security analysts always on the lookout for problems that put your security at risk. Our industry experts relentlessly monitor the ever-evolving security and threat landscape to maintain the latest knowledge about how infections happen. With that knowledge, Malwarebytes continuously improves the intelligence behind Trusted Advisor so that you always have the most proactive security measures to keep your data safe and private.

How is My Score Calculated?

Your protection score is comprised of two easy-to-read components that help you quickly assess how secure your device is.

- **Percentage:** a numerical score between 0% and 100%, where 100% is the best possible score, and 0% is the worst possible score.
- **Rating:** we eliminate all the guesswork by giving you an easy-to-read rating status that informs you whether your overall security is Poor, Fair, Good, Very good, or Excellent.

What Items Affect My Score?

Malwarebytes is committed to providing you with the best possible device security. We are continuously expanding and improving what Trusted Advisor monitors to cover you from all angles completely. The items we constantly inspect fall into six primary categories.

- **Real-Time Protection:** vital for keeping you safe from the most destructive threats and most common methods of infection.
- **Software updates:** keeping your apps up to date is one of the easiest and most important ways to improve your score. As cybercriminals are always finding weaknesses and vulnerabilities, keeping your apps up to date helps make sure you have the latest patches and security updates available to stay ahead of the game.
- **General settings:** checks for settings that may not be configured correctly within Malwarebytes, Windows, or your network preferences.
- **Device scans:** routine scans are an essential security best practice. Our Smart Scan technology makes scheduled scans more convenient than ever and only starts when your device is not in use. Trusted Advisor will notify you if you

get behind and need a reminder when it's time to scan again.

- **Online privacy:** taking a proactive stance on your privacy.
  - Block companies and websites from seeing your IP address and location to identify who you are, where you live, or what you do on the Internet.
  - Blocks third-party ad trackers that collect information about you by monitoring your online activity. This data is often shared and sold to marketing agencies exposing details about you that can be private or sensitive.
- **Device health: s**lowdowns in your device performance can be a real drag. Trusted Advisor helps you get the most out of your device so that you will never have to be left guessing whether malware is causing your device to grind to a halt.

Subscription Entitlement

Trusted Advisor also adapts to your subscription status to help you get the most out of your plan's protection components. No plan? No problem! For Free users, items requiring a Premium subscription are excluded from your score, giving you the best possible experience when using Malwarebytes and Trusted Advisor alongside another antivirus provider..

Issue Severity

The items are also assigned a severity based on the potential risk relevant to the issue. When problems are found, the quantity and severity of issues are considered when determining your score. Since high severity issues expose you to the most significant risk, having a single high severity issue will impact your score more than having multiple low or medium severity issues.

- High severity: 61% to 39% of your total score
- Medium severity: 30% to 10% of your total score
- Low severity: 9% to 3% of your total score

Details Page

To learn more and take action on problems found by Trusted Advisor, click the **See recommendations** button to be taken to a detailed overview page.

Status indicators

On the details page, items in a problem state will have a red indicator dot followed by a description of the issue. Many items also include an info tip to provide additional details about the issue and how it impacts your security. While an item is in a problem state, your protection score will be negatively impacted until the issue is resolved.

When an issue has been resolved, the indicator dot will change to green. Items with a green dot have a positive impact on your protection score.

Items appearing with a grey indicator dot do not impact your protection score. A grey dot is used to signify the item is either unavailable with your current subscription or intended for information purposes.

Customize Trusted Advisor

For advanced users, items monitored by Trusted Advisor can be ignored by clicking the '**x**' next to the item description. An item can only be ignored if it is currently in a problem state - items in a resolved state cannot be set to ignored. Once an item is ignored, it is placed in the Dismissed items section. The Dismissed items section is hidden by default and can be shown by clicking the Show dismissed items button at the top of the page. When an item is in the dismissed state, it is no longer factored into your protection score.

Manage Malwarebytes

Settings - Account

The Account tab allows you to view information related to your device, Malwarebytes version, and subscription. To view the Account tab,

1. Open Malwarebytes for Windows.
2. In the upper-right corner of the Dashboard, click **Settings**.
3. Click the **Account** tab.

Change or Deactivate License Key

Under the License key information, click **Change** or **Deactivate** your license key if you need to:

- Repair, replace, or sell your device
- Reinstall Malwarebytes
- Transfer the license key to another device
- Deactivate a premium subscription or premium trial to revert the program to the free version.

If you no longer have access to your device, see Deactivate device from your subscription.

Turn Auto-renewal Off/On

Under **Status**, if you have auto-renewal on, the remaining days until your next renewal displays. If you have auto-renewal off, the expiration date for your subscription displays. Click **Turn on auto-renewal** to open My Account in a browser window where you can enable auto-renewal for your subscription.

For more information, see Manage suto-renewal for your Malwarebytes subscription.

Change license key

This article guides you through changing your license key in Malwarebytes for Windows version 4.

1. From your desktop, click the **Malwarebytes** icon to open the application.
2. Click the **Settings** icon in the top-right corner.
3. Click the **Account** tab.
4. Click **Change**. The pop-up window offers the options to **Sign in** or **Enter license key** to activate your Premium subscription.
5. Click **Enter license key**. This opens the Activate License window.
6. Click the text box under **License key**, and enter your license key. Be sure to include hyphens and capitalization.
7. If you have a License ID, click the toggle next to **My license came with a License ID**.
8. Click the text box under License ID, then enter your ID.
    - **Important:** If you do not have an ID, do not click the toggle and continue to step 8.
9. Click the **Activate** button.

Deactivate Premium Trial

When you download Malwarebytes for Windows version 4 for the first time, you can provide your email to unlock Malwarebytes Premium features for 14 days. These features can be cancelled anytime during this time period. To deactivate your Premium Trial, follow these steps:

1. Open Malwarebytes for Windows.
2. Click the **cog** icon in the top-right corner.
3. Click the **Account** tab.
4. Under the License key field, click **Deactivate**.

When the Premium Trial has been deactivated, you can continue to use the free version of Malwarebytes for Windows to scan your computer for malware and disinfect your device after an attack. To prevent malware attacks before they cause damage to your computer, we recommend activating a Premium subscription for Real-Time Protection.on displays.

Enable Beta Updates

If you have an open ticket with us, the Support team may ask you to update to a beta version to resolve your issue.

Be aware:

- Beta software is sometimes provided by software providers as preview releases for quick bug fixes and access to new features.
- Beta software is not fully tested by Malwarebytes and may include significant issues.
- Malwarebytes strongly recommends you back up all of your data prior to using beta software from any source.
- Beta software is offered "AS-IS" and does not carry any warranties.

By default, the Beta updates toggle is off. Here are the steps to enable it:

1. Open Malwarebytes for Windows.
2. Click **Settings**.
3. In the General tab, scroll down to the **Beta updates** toggle.
4. Click the **Beta updates** toggle.
5. In the pop-up window, click **Enable Beta Application Updates**.

Manually Update your Database

Malwarebytes for Windows version 4 automatically performs database updates and scheduled scans. You can also manually update to the latest database version for your protections. There are two different ways to manually check for updates. See below for instructions on the method you prefer.

Check for Updates from Malwarebytes Dashboard

1. Open Malwarebytes for Windows.
2. Click the **Settings** button to the right. Then select the **About** tab to view the Version Information.
3. Click **Check for updates** to search for the latest Malwarebytes updates.

Malwarebytes for Windows will check for any protection database updates. This process may take a few moments.

Check for Updates from Windows Desktop

1. At the bottom right corner of your desktop task bar, click the up arrow to show hidden program icons.
2. Click the **Malwarebytes** icon. This will bring up a context menu.
3. Click **Check for Updates** in the context menu.
4. This will open Malwarebytes for Windows and check for any protection database updates. This process may take a few moments.

Quit the app

To stop Real-Time Protection, scans, updates, and other Malwarebytes for Windows version 4 Premium services, use the notification area to quit Malwarebytes. Services are programs that run in the background on your computer, even if the application is closed. If you quit Malwarebytes for Windows Premium, its services cannot start until you open the application or restart the computer.

1. In the system tray, click the **Show hidden icons** arrow.
2. The system tray is located on your taskbar next to your clock.
3. Right-click the **Malwarebytes** icon, then click **Quit Malwarebytes**.
4. When the User Account Control window appears, click **Yes**.
5. To restore your protection, open Malwarebytes for Windows Premium or use restart the computer.

Register the app with Windows Security Center

Windows Action Center is a notification and monitoring center available in Windows 7 and newer operating systems. Earlier versions of Windows offer similar services known as Windows Security Center.

Is Malwarebytes compatible with the Windows Security Center?

Malwarebytes for Windows version 4 did not appear in the Windows Security Center as a recognized security solution primarily due to the fact that Malwarebytes was not considered an Anti-Virus replacement or designed to register with this framework.

Malwarebytes for Windows version 4 now has the capability to register in Windows Security Center, allowing users to configure Malwarebytes as their primary security solution, or to run alongside their third party antivirus application.

Configure the Windows Security Center Setting for Malwarebytes

To configure Malwarebytes for Windows with the Windows Security Center:

1. Open the Malwarebytes for Windows application.
2. Click the Settings Capture2.PNGbutton on the right. Select the Security tab to locate Windows Security Center.
3. Toggle to enable or disable registering Malwarebytes with the Windows Security Center.

Uninstall the app

If you uninstall Malwarebytes for Windows version 4, you are no longer protected from threats like malware, potentially unwanted programs, and viruses. To uninstall Malwarebytes, follow these steps:

1. In your Windows desktop, click **Start**.
2. In the Windows search bar, search for **Control Panel**.
3. Click **Control Panel**.
4. Click Programs, select **Programs and Features**.
5. Locate Malwarebytes version x.x.x.xx on the program list.
6. Click **Malwarebytes version x.x.x.xx**.
7. Click **Uninstall**. The Uninstall Malwarebytes window displays.
8. In the Uninstall Malwarebytes window, select:
    - **Repair Malwarebytes:** If you're experiencing a technical issue, select this option to see an article with instructions on how to use the Malwarebytes Support Tool to uninstall and reinstall Malwarebytes for Windows while saving your setting configurations and subscription information.
    - **Remove Malwarebytes:** click this option to proceed with the uninstall process.
9. Follow the prompts to complete the desired actions.

Schedule and Run Scan

Scan a File, Folder, or External Drive

Not everyone stores their files on the local drives. A lot of us use external or portable drives to store sensitive data. We can scan them when they are plugged into our machines using two different methods. This article will show you how to scan external drives via the context menu entry and by scanning using a custom scan.

Option 1 - Right-click

1. Open the file manager (file explorer in Windows 10).
2. Right-click on the desired file, folder or drive to scan.
3. From the context menu, select **Scan with Malwarebytes**.
4. If on Windows 11, select **Show more options > Scan with Malwarebytes**.

Option 2 - Custom Scan

1. Open Malwarebytes on Windows.
2. Select the Scanner section on the main page, then click **Advanced scanners**.
3. Click on Configure Scan under Custom Scan, a new Windows shows the custom scan.
4. On the left side, you can configure options for the scan.
5. On the right side, you can select, files, folder or drives to scan.
6. Click **Scan** to start the scan.
    - **Note:** If you do not see your drive, use the right-click option. In some cases, Windows does not allow the display of the drive in our application.

During a custom scan, the scan time increases because all files and folder which are selected will be scanned. That means the scan is running much longer than a normal threat scan. Also, the usage of CPU and HDD can increase to 100% resulting in computer slowdown.

We suggest you perform a custom scan when you are not using the computer. The same is true when you enable the “scan for rootkits” option.

Scan Types

Malwarebytes for Windows version 4 provides three methods you can use to scan your computer: Threat Scan, Custom Scan, and Quick Scan. The scan method you choose determines how comprehensive of a scan Malwarebytes for Windows runs on your computer.

Threat Scan

Threat Scans detect threats in the most common system locations. If you have a paid subscription, a Threat Scan is scheduled to run once per week by default. Areas and methods tested include:

- **Memory Objects:** Memory allocated by operating system processes, drivers, and other apps.
- **Startup Objects:** Executable files or modifications that initiate at computer startup.
- **Registry Objects:** Configuration changes that may have been made to the Windows registry.
- **File System Objects:** Files stored on your computer’s local disk drives which may contain malware.

- **Heuristic Analysis:** Methods used by Malwarebytes in the previously described objects and other areas to detect and protect against threats and ensure those threats cannot reassemble themselves.

To run a Threat Scan

1. Click the blue **Scan** button.
2. To choose a scan method click the larger Scanner card.
3. The Scanner menu expands to present you with the Scan button.

Custom Scan

With a Custom Scan, you can choose what and where you want Malwarebytes for Windows to scan on your system. Depending on what locations you specify to be scanned, these scans can take a long time to complete. To avoid long wait times, we recommend you use Threat Scans unless there is a specific location on your device you want to scan.

To customize a scan:

1. Click the **Scanner** card.
2. Click **Advanced** scanners.
3. Click **Configure Scan**.

Custom Scan options

These settings allow you to determine the areas of your device you want Malwarebytes to scan. These are described as follows:

- **Scan memory objects:** Memory allocated by operating system processes, drivers, and other apps. Threats detected during scans are still considered threats even if they have an active component in memory. To be safe, memory objects should be scanned.
- **Scan registry and startup items:** Executable files or modifications that initiate at computer startup, as well as registry-based configurations that can alter your device's startup behavior.
- **Scan within archives:** If this box is checked, archive file types such as zip, 7z, rar, cab and msi are scanned up to two levels deep. Password protected archives cannot be tested.
- **Scan for rootkits:** Rootkits are files stored on your computer's local disk drives which are invisible to the operating system. These files may influence system behavior.
- **Potentially Unwanted Programs (PUPs):** This setting allows you to choose how Potentially Unwanted Programs are treated if detected. Use the drop-down menu to select either Ignore detections, Warn user about detections, or Treat detections as malware.
- **Potentially Unwanted Modifications (PUMs):** This setting allows you to choose how Potentially Unwanted Modifications are treated if detected. Use the drop-down menu to select either Ignore detections, Warn user about detections, or Treat detections as malware.

The right side of the Custom Scan screen also shows a list of directories and sub-directories to scan. By default, no directory is checked in a Custom Scan. You can check the box next to a directory; then, all sub-folders will automatically check for scan. You can un-check individual directories that you don't want scanned.

Quick Scan

Quick Scans check for threats in your Memory and Startup objects, where threats commonly take place. A Quick Scan is faster than a Threat Scan but less comprehensive. Only Malwarebytes Premium or Trial users can use this scan type. Areas and methods tested include:

- Memory objects: Memory allocated by operating system processes, drivers, and other apps.
- Startup objects: Executable files or modifications that initiate at computer startup.

If a Quick Scan detects malware, we strongly recommend running a Threat Scan afterward in case of more threats in other areas of your device. By default, any threats detected during a scan are quarantined. For information on Quarantine, see "Restore or delete quarantined items."

If you have the paid version of Malwarebytes for Windows installed, you can schedule a Threat, Custom, or Quick Scan to run automatically. For instructions, see "Set up automatic scans."

Set Up Scheduled Scans

With a paid subscription, you can schedule times for scans to run automatically in Malwarebytes for Windows version 4. When you activate your subscription, a Threat Scan is scheduled to run daily. You can edit or delete scheduled scans, and add new scans to run at your preferred time by going to the Scan Scheduler screen. Scheduled scans are not available for the Malwarebytes Free version.

Optimize your Scan Schedule

After the first scan, new users are prompted to select the time of the next scan, which updates the default time of the scheduled scan.

1. In the Threat Scan summary window, click **Next**.
2. The scan scheduling pop-up window displays. Select the time for your next scan: Daily, Weekly (recommended), or Monthly.
3. On the top right, toggle-on **Use smart scan** if you want the scan to start when the device is idle.
4. Click **Save** to apply your selection. You're taken back to the Threat Scan summary window.

Add or Edit Scheduled Scans

The Scan Scheduler lets you add, edit, or delete scheduled scans as needed.

1. Open **Malwarebytes**.
2. Click the **Scanner** card, then click the **Scan Scheduler** tab.
3. Choose to add or edit a schedule.
   - To schedule a new scan, click **Schedule scan**.
   - To edit an existing scan, hover your cursor over the scheduled scan and click the pencil icon.
4. If adding a new scheduled scan, Malwarebytes prompts you to select a Threat Scan, Quick Scan, or Custom Scan before presenting edit options. If editing an existing scheduled scan, Malwarebytes presents you with the edit options for that scan type. Use the menu to configure your scheduled scan.
5. For additional options for Threat Scans and Quick Scans, click **Advanced**. Custom Scans offer advanced options upfront. Depending on the scan type, you will see some or all of the options described:
   - **Quarantine all threats automatically:** Check this box if you want Malwarebytes to quarantine detected threats without asking you. This setting may allow Malwarebytes to mistakenly quarantine programs that are not threatening, also known as a false positive detection.
   - **Restart computer if needed to remove threats:** This is available only if threats are automatically quarantined, and is not checked by default. This setting allows Malwarebytes to automatically restart your device if needed for remediation without a window prompt.
   - **Scan memory objects:** Check this box if you want Malwarebytes to scan memory allocated by operating system processes, drivers, and other apps.
   - **Scan registry and startup items:** Check this box if you want Malwarebytes to scan executable files or modifications which initiate at computer startup.
   - **Scan within archives:** This box is checked by default. This allows scanning to go two levels deep within archive files.

- **Scan for rootkits:** Check this box if you want Malwarebytes to look for rootkits on your device. This makes the scan take longer.
- **Notify me when a scan completes, only if items are detected:** Check this box if you want to disable notifications for Scans complete when nothing is detected.

6. If missed, scan at next opportunity: Keep this switch turned on if you want Malwarebytes to run a scan at the next available opportunity if the scheduled scan was missed because your device was off or asleep.

7. Use smart scan: Keep this toggled on if you want the scan to start when the device is idle.

8. To confirm your scan configurations, click **Schedule**.

9. For Malwarebytes for Windows to scan your computer, your computer must be turned on and awake. If a scan is missed or stopped because the computer goes to sleep or is turned off, the scan resumes when the computer is turned on.

Manage Threats

Real-Time Protection

Paid subscribers of Malwarebytes for Windows version 4 gain access to multiple protection layers which actively stop threats. The Real-Time Protection card shows you each protection layer, switches to turn the features on or off, and protection statistics.

Protection Layers

The Real-Time Protection card on the Dashboard displays each of the protection layers. You can click on the switches for any of the protection layers to toggle them on or off. We recommend keeping them on to remain fully protected by Malwarebytes. Each protection layer is described here:

- **Web Protection:** This layer protects you from online scams, phishing sites, and sites containing ransomware.
- **Malware & PUP Protection:** This layer blocks malware, viruses, adware, potentially unwanted programs (PUPs), and other threats.
- **Ransomware Protection:** This layer blocks malware that locks you out of your device and files, which then demands payment to restore access.
- **Exploit Protection:** This layer blocks malware which seeks to leverage bugs and vulnerabilities in a system to allow the exploit's creator to take control.

Click the Real-Time Protection card from the main program Dashboard to view more information.

Items Stopped in Last 30 Days

Once you click and expand the Real-Time Protection card, the left side of the Real-Time Protection screen displays all the threats Malwarebytes prevented in the last 30 days.

- Select the **My Computer** tab to see the total threats stopped on your device, and the breakdown of each threat type prevented, including Real-Time Protection and Browser Guard detections. Browser Guard data is available when the extension is installed on your default browser (available for Chrome, Edge, and Firefox).
- Select the **Global** tab if you want to view how many threats Malwarebytes for Windows has stopped around the world in the last 30 days.

Check your Real-Time Protection status

Real-Time Protection is a feature available in Malwarebytes for Windows version 4 and other Security & Antivirus products. Depending on your operating system, Real-Time Protection can block malware, exploits, ransomware, or malicious websites. To check if Real-Time Protection is on or off, open the Malwarebytes application and view your Dashboard or refer to the instructions below.

Check Real-Time Protection in Malwarebytes for Windows:

1. Open Malwarebytes for Windows.
2. See the right-hand side of the Malwarebytes Dashboard to see which protection is enabled or disabled.
3. Real-Time Protection is more effective with all protection layers turned on. If any Real-Time Protection layers are turned off, we recommend turning them on as soon as possible. For more information, see "Real-Time Protection."

View Reports and History

When Malwarebytes for Windows version 4 blocks a website or exploit on your computer, or a Real-Time Protection detection happens, the event is logged and a report is created. You can review the details of each Malwarebytes scan or detection, and what threats were identified. Reports are stored up to the last 30 days. You can view the reports in the Malwarebytes program, copy the report to your Clipboard, or download a Text file (.txt).

View and Download Scan Reports

Scan reports contain all of the information and details on executed scans. To view and save your scan reports:

1. Open Malwarebytes for Windows.
2. Click the **Scanner** card.
3. Click the **Reports** tab.
4. At the top-right of the Scan reports, you can **Hide reports with no detections** by checking the box.
5. Hover your cursor over the report you want to view and click the **eye** icon.
6. A Summary window displays to show the scan results and the date and time executed. For more details, click the **Advanced** tab in this window.
7. If you want to download the full report, click **Export**, and click either **Copy to Clipboard** or **Export to TXT (*.txt)**.
8. You can sort the Reports list by Type or Date by clicking on the column headers.

Remove any report in this list by hovering your cursor over the report and clicking the **trash** icon. To remove all of the reports in this list, click the menu icon in the list header, then click **Delete all**.

View and Download Detection History Reports

The History tab lists Real-Time Protection (RTP) and scan detections. Anytime Real-Time Protection blocks malicious sites or software, or anytime Malwarebytes scans detect malicious items, a report generates on this screen. To view and save your History reports:

1. Open Malwarebytes for Windows.
2. Click the **Detection History** card.
3. Click the **History** tab.
4. Hover your cursor over the report you want to view and click the **eye** icon.
5. A Summary window displays to show the threat details, the protection date and time, and the action executed. For more details, click the **Advanced** tab in this window.
6. If you want to download the full report, click **Export**, then click either **Copy to Clipboard** or **Export to TXT (*.txt)**.

Remove any report in this list by hovering your cursor over the report and clicking the **trash** icon. To remove all of the reports in this list, click the menu icon in the list header, then click **Delete all**.

Manage the Allow List

Malwarebytes for Windows version 4 can block items, including websites, applications, and files, that are not inherently malicious. The most common non-malicious detections are Potentially Unwanted Programs (PUPs) and Potentially Unwanted Modifications (PUMs).

There may be occasions when Malwarebytes for Windows flags items as malicious, but you want to keep them on your device. Add the item to your Allow List to stop Malwarebytes for Windows from blocking 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. In Malwarebytes for Windows, there are four types of exclusions you can add:

- File or folder
- Website
- Application that connects to the Internet
- Previously detected exploit

Add Item to the Allow List

1. Open Malwarebytes for Windows.
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 type of exclusion you want to add:
    - **Allow File or Folder:** Click Select a file or Select a folder. Choose the file or folder you wish to exclude, then click Open. Under Exclusion rules, choose how you would like to exclude the file or folder.
    - **Allow a website:** Click on the text field under Add a URL or Add an IP Address. Enter the URL or IP Address in the text field.
    - **Allow an application to connect to the Internet:** To find the application, click Browse. Select the application executable you want to add, then click Open.
    - **Allow a previously detected exploit:** Applications with an identified exploit are listed on this screen. Check the box next to the exploit you want to allow.
6. Click **Done** to confirm your changes.

Once an exclusion is added to Malwarebytes for Windows, the exclusion begins to take effect immediately.

Remove an Item from the Allow List

Removing an item from the Allow list allows Malwarebytes to detect it again. This is helpful if you decide you no longer want to exempt the item from scanning.

1. Click the **Detection History** card.
2. Click the **Allow List** tab.
3. Hover over the item you want to remove, then click the **trashcan** icon.

Potentially Unwanted Modification Blocks

Malwarebytes for Windows version 4 detects Potentially Unwanted Modifications (PUMs) to help prevent software from making unauthorized changes to the Windows settings on your computer. PUMs are not always harmful, but they can change the way your computer behaves. You can research more about PUMs on our blog, Malwarebytes Labs.

PUMs can prevent you from doing common tasks such as:

- Opening your Start Menu
- Performing updates
- Viewing File Explorer
- Using Task Manager

When PUM is detected on your computer, Malwarebytes for Windows does not know whether or not it was authorized. Optimization software, malware, and Potentially Unwanted Programs (PUPs) are known to make these types of changes, hence they are regarded as potentially unwanted.

To have Malwarebytes for Windows ignore a PUM, you must add the PUM as an exclusion.

1. Open Malwarebytes for Windows.
2. Click the **Settings**, then select the **Security** tab.
3. Scroll down to **Potentially unwanted items**.
4. In the drop down next to Detect Potentially Unwanted Modifications (PUMs), select **Ignore Detections**.
5. Turning this setting off prevents Malwarebytes for Windows from quarantining the PUM automatically.
6. Go to the Dashboard, then click **Scan**.

When a PUM is excluded, Malwarebytes for Windows does not detect the PUM during scans or Real-Time Protection. To add, edit, or delete exclusions, refer to “Manage the Allow List”.

Web Protection Blocks

If Malwarebytes for Windows version 4 displays a website blocked notification, this indicates Web Protection has blocked a potentially harmful website that may infect your computer. If you have encountered a website blocked notification, we recommend you scan your device to ensure your not infected.

The website blocked notification above shows the following information:

- The website’s Domain.
  - A domain refers to the name of the website, such as www.malwarebytes.com.
  - Excluding a domain may not exclude all parts of a website.
- The website’s IP address.
  - An IP address is a unique, numeric set of numbers devices use to communicate with each other.
  - Excluding an IP address may exclude the entire website domain.
- Which port the website used.
  - Port numbers help identify what type Internet activity was used.
  - Knowing the type of Internet activity can help isolate the cause of the issue.
- Whether the website was inbound or outbound.
  - Outbound: a file or process on the device attempted to contact a malicious IP address.
  - Inbound: a malicious IP address attempted to contact the device.
- The file (or process) on the device that was used to contact the website.

- Internet activity is often transferred using files on your device.
- Files are commonly associated with Internet applications such as browsers or peer-to-peer (P2P) clients.
- Excluding a file or process may allow all Internet activity to pass through the respective application.

If you continue to receive Website Blocked notifications after running a scan with Malwarebytes, please contact Support so we can assist in isolating and removing the source of the website block. To prevent Web Protection from blocking a website you trust, refer to the article Manage the Allow List.

Verify Web Protection is Working

If you have accessed a website you feel Malwarebytes for Windows version 4 Premium should have identified as "malicious", verify Web Protection is working. When Web Protection is turned on and working, Malwarebytes for Windows Premium intercepts malicious websites and displays a notification.

Malwarebytes for Windows may not block a website if:

- Web Protection is turned off
- the website is not known to contain malware
- another antivirus is installed on your computer
- Verify Web Protection is working

If Web Protection is turned on, you can test the protection module to see if it is working. To confirm Web Protection is turned on, see "Check the Real-Time Protection status."

1. Open your Internet browser.
2. In your browser's address bar, enter the website address http://iptest.malwarebytes.com/. This website address is used to test Web Protection on your computer. It is not a malicious website.
3. If Web Protection is not working, the website displays the following message: **IF YOU ARE ABLE TO REACH THIS PAGE IT MEANS THAT IP PROTECTION IS DISABLED ON YOUR MACHINE.**
4. If Web Protecting is working properly, the following message and notification appear: **Website blocked due to malware**
5. If Web Protection is not working and you have another antivirus installed, consider adding Malwarebytes to the other antivirus' exclusions. For more information, refer to Malwarebytes for Windows antivirus exclusions list.
6. If Web Protection is working, see Submit a phishing link, malicious website, or file to Malwarebytes.

Repeated Chrome Detections

To check if Malwarebytes for Windows version 4 is detecting a recurring Google Chrome™ browser item, follow these steps:

1. From your Malwarebytes for Windows dashboard, click the **Scanner** card.
2. Click the **Reports** tab to display your previous scans.
3. Double-click a **Scan Report**.
4. Check the listed items in the scan report to confirm if a Chrome item is repeatedly detected.

Malwarebytes is removing the detected item, but the Google Sync server restores the item back. For more information, see our forum topic, Chrome Secure Preferences detection always returns.

1. To prevent the same items from coming back to your device, reset Chrome Sync.
2. Turn Chrome Sync off. See the following Google support article: Turn sync on and off in Chrome.

3. Sign in to https://chrome.google.com/sync.
4. Scroll down and click **CLEAR DATA**.
5. After performing the sync reset, return to Malwarebytes and close the Additional action required popup message to resume the quarantine process.
6. After the quarantine process, turn Chrome Sync back on. Refer to the steps in Google's support article: Turn sync on and off in Chrome.

"Website blocked due to compromise" Message

This is an incoming block - meaning the IP address you see us blocking is scanning and/or attempting to force its way into your machine via different ports. These attacks can last anywhere from a few hours, days, to a week. They probe IP ranges then attempt to brute force their way into machines in order to infect them with ransomware.

The most common method of accessing machines is via Windows Remote Desktop Protocol (RDP). We recommend you check to see if you have the Remote Desktop enabled and if so, disable it. For more information, see How to use Remote Desktop.

If you need to use Remote Desktop, see our Malwarebytes Labs article How to protect RDP on how best to lock it down.

What you can do:

- Given that Malwarebytes is blocking the attackers, you do not need to worry and no further action is required.
- If the block alerts are interfering too much with your daily work, it may help if you add the IP address you see in our Alert to the Windows Firewall. To view the IP address in our alert:
    1. Open Malwarebytes for Windows version 4 > click the **Detection History** card.
    2. Click the **History** tab.
    3. Under the Event column, open the Real-Time Protection detection report.

Troubleshooting

Internet Browser Issues on Windows

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 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.

Unwanted 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.

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.

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 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.

Issues Running other Security Applications

Malwarebytes Web Protection blocks traffic from domains and IP addresses that could infect your device with threats like trojans, potentially unwanted programs, and viruses. When Web Protection and a third-party application that uses the Windows Filtering Platform (WFP) are enabled on your device, the following issues may occur:

- Blue screen of death (BSoD)
- Loss of Internet
- Loss of the third-party application's functions

These issues occur because both applications are using the WFP. You must either disable your third-party application or the Malwarebytes Web Protection feature.

Disable Third-party Application

Issues have been reported when Malwarebytes' Web Protection is enabled and the following third-party applications are running:

- AdGuard
- Avast™ antivirus products
- AVG™ antivirus products
- BitDefender™ AV products
- Emsisoft Anti-Malware
- Firetrust HideAway VPN
- Kaspersky™ anti-virus products
- NordVPN™ Threat Protection
- Private Internet Access
- Qustodio
- Sophos anti-virus products
- SurfShark
- Techloq Filter

Disable Malwarebytes Web Protection

If you are encountering issues, you may disable Web Protection. Disabling Web Protection means the real-time protection layer no longer blocks traffic from domains and IP addresses that could infect your device. To disable Web Protection, follow these steps:

1. Open Malwarebytes for Windows.
2. In the Real-Time Protection card, click the **Web Protection** toggle.
3. In the User Account Control pop-up window, click **Yes**.

If you have the Alert me if any Real-Time Protection modules are turned off notification toggle turned on, Malwarebytes notifies you that you have one of the Real-Time Protection layers turned off. To disable this setting, see "Settings -Notifications."

Malwarebytes Blocks System Restore

If you run System Restore on a computer with Malwarebytes for Windows version 4 installed, you may encounter an error message.

To resolve this conflict, disable the Malwarebytes for Windows self-protection feature and quit Malwarebytes for Windows.

Disable Self-protection

1. Open Malwarebytes for Windows.
2. Click **Settings** on the right. Then select the **Security** tab.
3. Scroll down to Windows Startup, then select **Advanced**.
4. Toggle off **Enable self-protection** module.
5. When the User Account Control window appears, click **Yes**.
6. See the instructions below to quit Malwarebytes for Windows.

Quit Malwarebytes for Windows

1. Click the Show hidden icons arrow to display your hidden notifications.
2. Locate the Malwarebytes logo and right-click the icon.
3. Click **Quit Malwarebytes**.
4. Run **System Restore** again.
5. When you finish running System Restore, turn self-protection back on to protect Malwarebytes for Windows.

Note: If you are still encountering the System Restore error, there may be another anti-virus installed on your computer. Check with the other anti-virus vendor for a resolution.

Malwarebytes Making DNS Queries for Excluded Domains

If you are using a program to monitor your network traffic, the program may show data for a computer with Malwarebytes for Windows installed that is making multiple DNS queries for websites in their exclusions list. Refer to "Add item to the Allow List" to set up exclusions in Malwarebytes for Windows version 4.

This is expected behavior. When you set up a website exclusion in Malwarebytes for Windows, you have the option to Exclude a domain or Exclude an IP Address. When exclude a domain is selected, Malwarebytes for Windows will query for the IP address of the excluded domain so it can also add the IP address to the Allow List.

Malwarebytes for Windows v4 Support for Windows 7

Malwarebytes for Windows version 4 is committed to continue support for Windows 7 for as long as Microsoft allows us to. This stand means that we'll continue offering our core anti-malware protection to the best of our ability, given technical limitations.

SSL Protocol Error in Google Chrome

While running the Malwarebytes Antivirus & Security version 4 program on your Windows device, Google Chrome™ browser reports an SSL_Protocol_Error when navigating to websites blocked by Malwarebytes.

Symptoms

- Navigating to websites that are blocked by our software produces an SSL_Protocol_Error in Chrome.
- Occurs while the Web Protection toggle is switched on.

Environments

- Operating systems: Windows 7 and newer
- Browsers: Google Chrome version 90-94
- Malwarebytes products: Malwarebytes for Windows

Workaround

While we investigate this issue to find a permanent resolution, you can clear Google Chrome's cache to resolve this issue. For more information, see Clear Cache & Cookies in Google Chrome.

Support Tool

Malwarebytes Support Tool FAQs

The Malwarebytes Support Tool is designed to help you troubleshoot issues with Malwarebytes for Windows version 4. The Malwarebytes Support Tool combines multiple utilities, such as the Malwarebytes Cleanup Utility and Farbar Recovery Scan Tool. The Malwarebytes Support Tool gathers information from your computer and updates an existing ticket with the information gathered.

Download the latest version of the Malwarebytes Support Tool, then open the utility and accept the license agreement. For further instructions, refer to Uninstall and reinstall Desktop Security with the Support Tool.

What can the Malwarebytes Support Tool do?

- Provide self-help options to assist with troubleshooting
- Attach information to an existing Malwarebytes Support ticket
- Automatically generate and upload information to a secure Malwarebytes server
- Automatically run troubleshooting tools, including:
  - Farbar Recovery Scan Tool (FRST)
  - Malwarebytes Cleanup Utility (MB-Clean)
  - MB-Check
  - MB-Grab
- Function using an online or offline mode
- Advanced Options
  - Allows you to use the Malwarebytes Support Tool without an Internet connection
  - Saves troubleshooting logs to your computer
  - Uninstalls Malwarebytes for Windows using the Cleanup Utility

Do I need a license for the Malwarebytes Support Tool?

No, the Malwarebytes Support Tool is a free troubleshooting and repair utility. You may download and run the Malwarebytes Support Tool as needed.

How do I upload logs to an existing Support ticket?

If you have an open ticket with Malwarebytes Support, enter your ticket number and email address when prompted in the Malwarebytes Support Tool. For instructions, refer to the article Collecting logs with the Windows Support Tool.

What is the mbst-grab-results.zip file?

mbst-grab-results.zip is an archive that contains results from running the Malwarebytes Support Tool. Inside the mbst-grab-results.zip file, there are two logs:

- mb-support-log.txt file - contains the Malwarebytes Support Tool data and any exceptions the application encountered.
- mb-check-results.txt - contains data to help us troubleshoot issues with Malwarebytes for Windows.

If the Malwarebytes Support Tool is run in offline mode, the mbst-grab-results.zip file is saved to your desktop.

Do I still need to run other troubleshooting or repair tools?

With the Malwarebytes Support Tool, you do not need to run additional troubleshooting or repair tools, such as the Malwarebytes Cleanup Utility.