

Malwarebytes

**ENDPOINT
SECURITY**

**Mac Remediation Client
Administrator Guide**

Version 1.3.1
27 September 2017

Notices

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

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

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

Copyright © 2017 Malwarebytes. All rights reserved.

Third Party Project Usage

Malwarebytes software is made possible thanks in part to many open source and third party projects. A requirement of many of these projects is that credit is given where credit is due. Information about each third party/open source project used in Malwarebytes software – as well as licenses for each – are available on the following page.

<https://www.malwarebytes.com/support/thirdpartynotices/>

Sample Code in Documentation

The sample code described herein is provided on an "as is" basis, without warranty of any kind, to the fullest extent permitted by law. Malwarebytes does not warrant or guarantee the individual success developers may have in implementing the sample code on their development platforms. You are solely responsible for testing and maintaining all scripts.

Malwarebytes does not warrant, guarantee or make any representations regarding the use, results of use, accuracy, timeliness or completeness of any data or information relating to the sample code. Malwarebytes disclaims all warranties, express or implied, and in particular, disclaims all warranties of merchantability, fitness for a particular purpose, and warranties related to the code, or any service or software related there to.

Table of Contents

About the Mac Remediation Client	1
What's New	1
System Requirements	1
End-User License Agreement (EULA).....	1
External Access Requirements.....	1
Installation	2
How to use the Mac Remediation Client.....	4
Scan	4
Special Cases	5
Optional items	6
Compromises.....	6
Next Steps.....	6
Gathering Information about Your System.....	7

About the Mac Remediation Client

The Mac remediation client is an application for macOS designed to remove malware and adware from your endpoint. It is very simple to use, and for most problems, should clean up your system in less than a minute, *from start to finish*. Just open the app, click the Scan button, and remove anything that is detected. That's it!

The Mac remediation client is an app that should be provided by your business' IT department, along with a license key. If you have received this app from a different source and need a license key, see the *Malwarebytes Endpoint Security* page on our website for more information.

What's New

The following changes have been incorporated in this version of *Malwarebytes Breach Remediation*.

- Added ability to handle larger threat signatures
- Fixed scan engine so that disconnected network drives assigned as login items do not affect scan integrity
- Improved High Sierra compatibility
- Fixed a bug that could cause the program to be unable to scan
- Other internal bug fixes

System Requirements

Following are minimum requirements for an endpoint on which the Mac remediation client may be installed. Please note that these requirements do not include any other functionality that the endpoint is responsible for.

- **Operating System:** macOS version 10.9.5 or later.
- **Security & Privacy:** Allow apps to be downloaded from Mac App Store and identified developers (most restrictive setting)
- **Active Internet Connection**

End-User License Agreement (EULA)

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

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

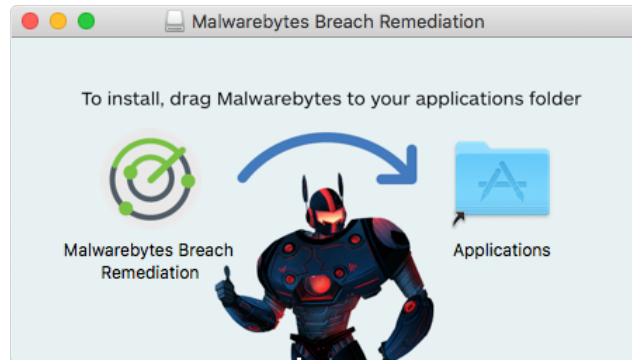
External Access Requirements

If your company's Internet access is controlled by a firewall or other access-limiting device, you must grant access for the Mac remediation client to reach Malwarebytes services. These are:

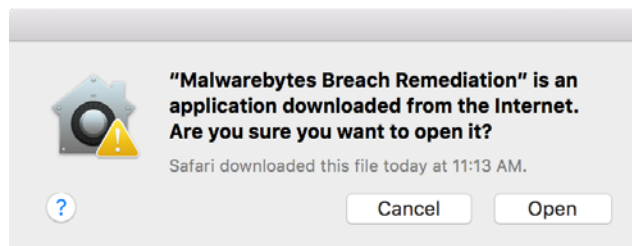
https://data.service.malwarebytes.org	Port 443	outbound
https://data-cdn.mbamupdates.com	Port 443	outbound
https://*.mwbsys.com	Port 443	outbound

Installation

When you download the Mac remediation client, you will receive a file named **MBBR-Mac-<version>.dmg**, where <version> is the version of the downloaded file. Open that file, and you will see a window prompting you to install the Mac remediation client by dragging it into the Applications folder.



After doing this, go to the Applications folder and open the Mac remediation client. The first time you open it, you should see a window asking you if you're sure you want to open it. Click the **Open** button.

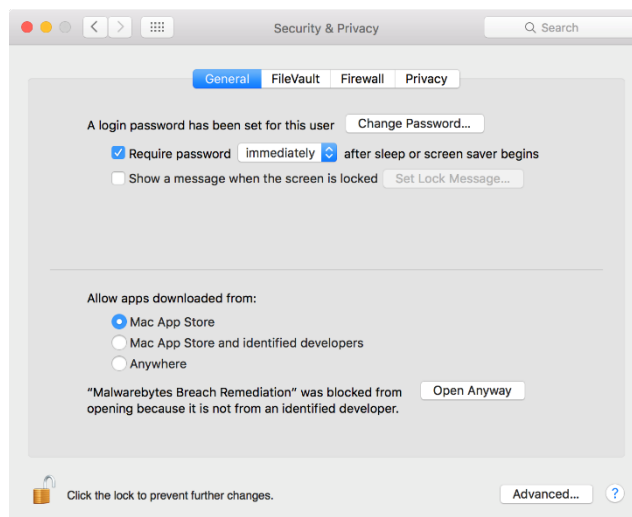


It is possible you will see this window instead:



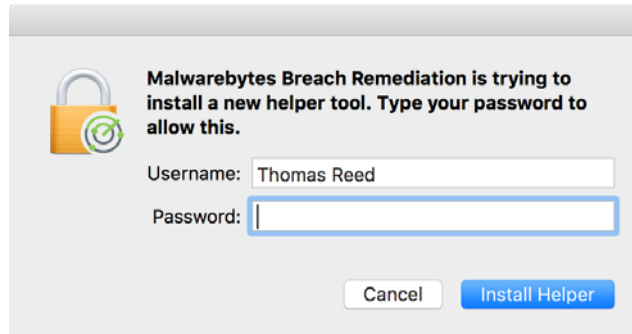
If that is the case, your security settings are set to allow only apps downloaded from the Mac App Store. To open the Mac remediation client, go to System Preferences and click the **Security & Privacy** icon.

In the Preference pane, click the **Open Anyway** button to allow the app to open. You could also unlock this pane by clicking the lock icon in the bottom left corner and entering your password, then changing this setting to "Mac App Store and identified developers," which will allow the app to open normally. **Please note:** It is not advisable to change this preference to "Anywhere" unless you know exactly what you're doing!



Once opened for the first time, the app will ask for an admin password to install a helper tool.

This tool will be used to remove adware or malware that has been installed into locations that require a higher privilege level to access. Without this helper tool, the Mac remediation client will not be able to remove all adware and malware.



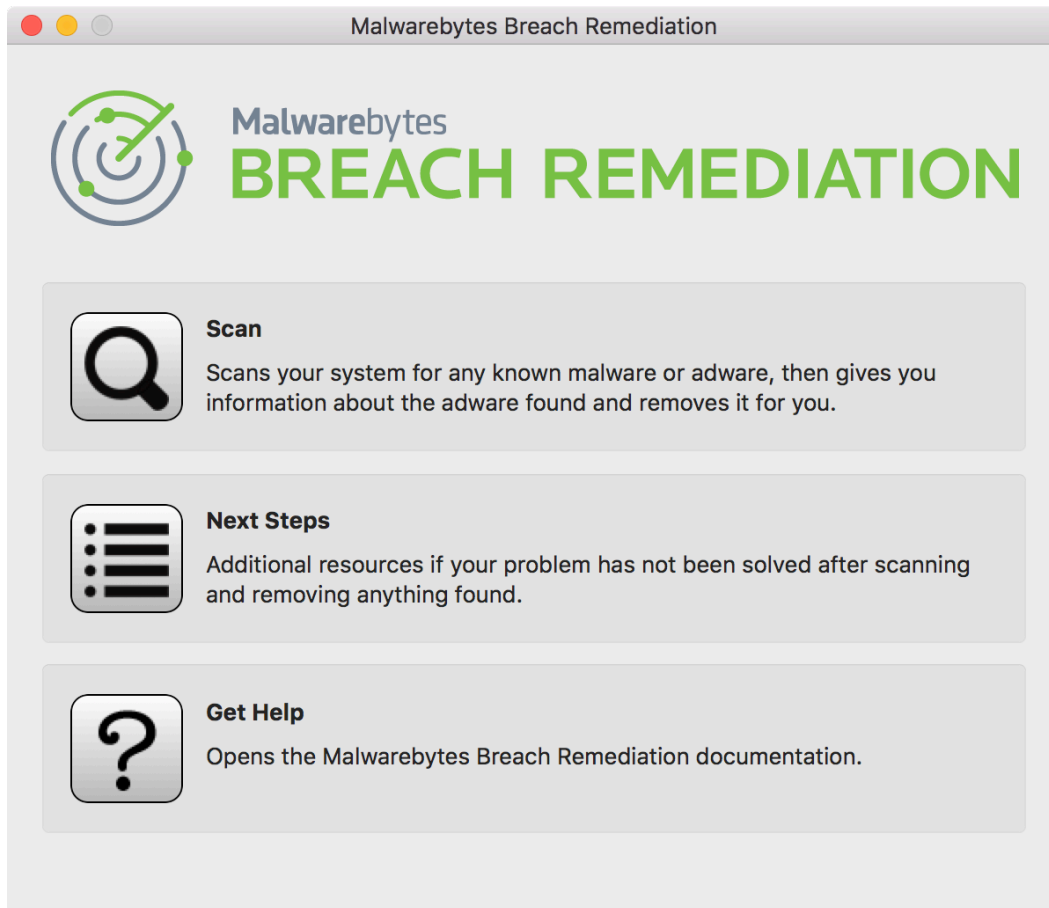
Installation of the helper tool may need to be repeated again at some point in the future, if the tool is deleted or if a newer version becomes available.

In addition to the helper tool, the Mac remediation client will add an item named "**com.malwarebytes.services**" to the keychain during installation. This is used to store data which identifies your system to our update servers, and is a pre-requisite for downloading of database updates. This is not something you will be aware of unless you go looking for it, and be aware that adding an item to the keychain does not mean that the app has access to anything else in your keychain; it does not.

If you wish to remove the Mac remediation client, as well as the helper tool and all data and settings files, simply open the Mac remediation client and choose **Uninstall Malwarebytes Breach Remediation** from the [Help](#) menu.

How to Use the Mac Remediation Client

When you open the Mac remediation client you will see that it has a very simple interface:

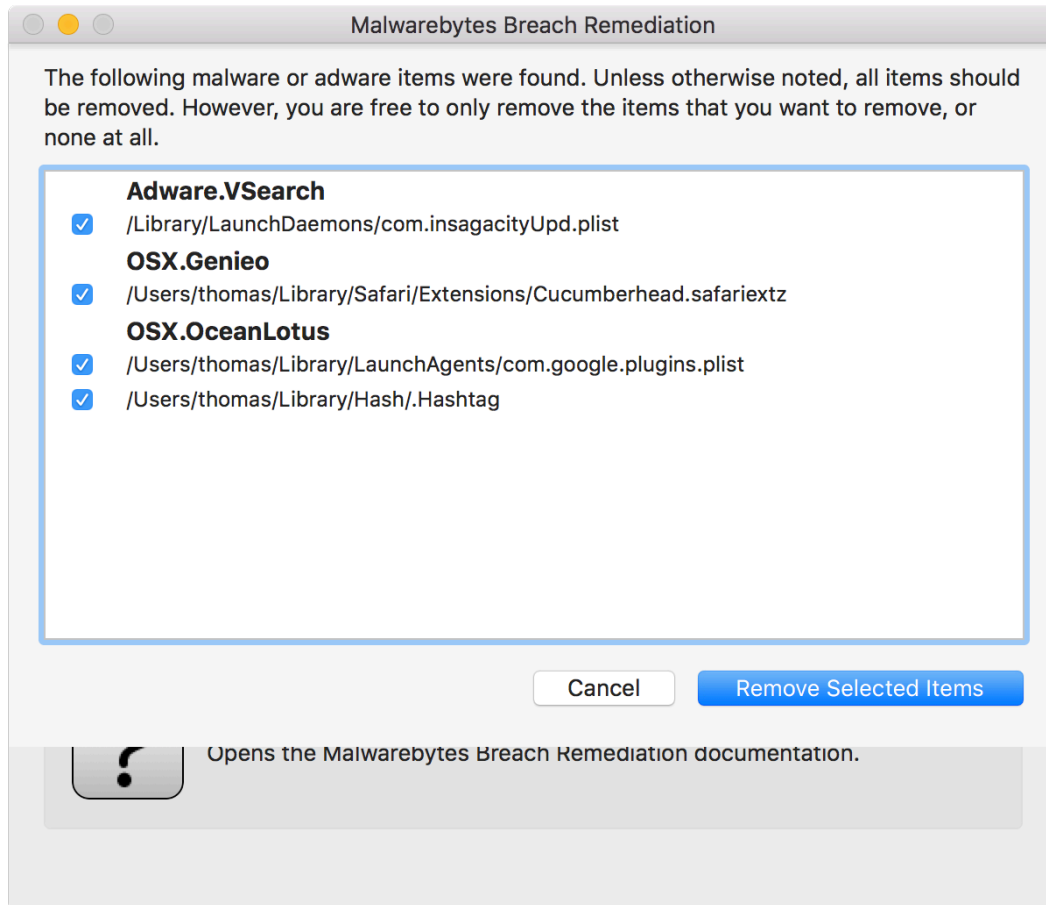


In the background, the Mac remediation client has also checked in with Malwarebytes to check for signature updates. This is the only time that the program automatically checks for updates. You can also check for updates manually by selecting **Update Signatures** from the **Scanner** menu. You can find the database signature version number as well as the program version by selecting the **About** screen.



Scan

Click the **Scan** button to immediately scan your Mac for malware and adware. The scan should be very quick, and is completely safe, as nothing will be deleted yet. After the scan finishes, if your system is clean, you will be told that nothing was found. Otherwise, a window will open showing what was detected:



The screenshot above shows that components of Conduit, Genieo and VidX (aka MacVX) were found, and reveals where the problem files can be found. If the full path to the file cannot be seen, you can hover the mouse over a detected item to get a “tooltip” window showing the full path.

The checkboxes allow you to specify which items are to be removed. (By default, only files that are definitively bad will be checked.) Clicking the **Remove Selected Items** button will remove any items that are checked, and will leave any that are not checked in place.


Removal of some items will require entry of your admin password. Rest assured, the password request is provided by Mac OS X, and the Mac remediation client will never actually see your password. If you choose not to enter your password, all items that do not require admin permissions will be removed, but those that do need higher permissions will be left in place. They will need to be removed manually, or by a subsequent scan in which you provide the password.

If you installed the program on a non-admin user account, you will need to provide both an admin username and password when asked. As long as you do this, the detected items can be removed just as well from a non-admin account as from an admin account. There is no need to log in to a different account.

If the program was installed on a different user account, you will need to log in to that account to fully remove all components of some malware or adware.

Files that are removed are not deleted outright. Instead, they are moved to a folder named “Malwarebytes Removals” in the trash can. This allows you to examine them and delete them at your leisure, or replace items that may have been removed by mistake.

Special Cases

There are a couple special cases to be aware of, denoted in the detection list by a  symbol on the right edge of the list. If you hover the mouse over that symbol, you will get a short explanation in a pop-up tooltip.

Optional Items

These are legitimate files – such as web browser preference files – that may have been modified. For example, some adware has been seen to insert custom JavaScript code into Firefox’s preference file. These items can be removed, but since that may result in loss of things like browser settings, they are not checked by default.

Compromises

Some malware and adware is known to make modifications that may require more intensive work to fix. In such cases, a window will pop up informing you about the problem and providing a link where you can read more about what to do next.

Next Steps

If you have scanned your endpoint with the Mac remediation client, removed everything that was detected and restarted the endpoint (if instructed to do so), and you are still having a problem, click this button. It will open a window that loads the following page from the Malwarebytes website that contains up-to-date information about what to try next.

https://support.malwarebytes.com/customer/en/portal/articles/2401953-?b_id=6401

Because most computer problems are not the result of malware or adware, it is entirely possible that the Mac remediation client may not solve all your problems. This page will help you try to find and solve other issues.

Gathering Information about Your System

To get a profile (“snapshot”) of your system, simply choose **Take System Snapshot** from the Scanner menu. This will open a window showing just the system information and nothing else. You can feel free to copy any of the text from this window or choose **Save** from the File menu to save the snapshot to a text file on your hard drive.

This feature can be helpful for techs who are trying to troubleshoot a problem with your endpoint, or for times when you’re posting to a forum about a problem you’re having and need to provide some contextual information, or any number of other uses.