Malwarebytes
BREACH
REMEDIATION

Malwarebytes Breach Remediation (Mac) Command Line Administrator Guide

Version 4.15.0

5 August 2022

Notices

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://service.malwarebytes.com/hc/en-us/articles/4414986433683

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.

The Malwarebytes Protection Strategy

Malwarebytes products incorporate several prevention features which utilize a layered defense strategy to protect you against malware threats which you face daily. Each layer is designed to disrupt the attack chain at a different stage. While all Malwarebytes products are highly effective in dealing with attacks that are becoming all too commonplace, our protection capabilities are most effective when you take advantage of the full product suite, allowing each prevention layer to do the job they are best suited for.

It’s your data. Protect it wisely!

CMB18-1031a

Table of Contents

Introduction 1
- What's New 1
- Key Features 1
- System Requirements 1
- External Access Requirements 1
- Remote Operations 2

Using Malwarebytes Breach Remediation 2
- Manual Deployment 2
  - Deployment 2
  - Execution 2
  - Grant Full Disk Access 2
- Activate License 3
- Remediation Now or Later? 3
  - Diagnostic Scan 4
  - Remediation Scan 4
  - Scan Output 4
  - Quarantine Output 4
- Restoring Items from Quarantine 5

Command Line Parameters 5
- Conventions 6
- Command Line Overview 6
- Command Line Reference 6
  - version 7
  - license 7
  - scan 8
  - status 8
  - update 9
  - quarantine 9
  - uninstall 10

Introduction

Malwarebytes Breach Remediation is designed to allow business users to detect and remove malware from endpoints. It is built upon the power of our *Malwarebytes* client.

Implementation in a command line form provides increased flexibility for IT staff to deploy the client, detect and remediate threats, gather activity logs, and continue with their daily tasks – all with a minimal investment in time and resources quickly and easily.

What's New

Malwarebytes Breach Remediation 4.14 is a complete overhaul on the previous versions, bringing it up to date with the latest components of our engine and software. As such, the software has changed, both with how it's installed and executed with the command line usage. Please read this guide carefully for full details.

Key Features

Malwarebytes Breach Remediation offers the following key features:

- Access Malwarebytes functionality via a non-persistent command line utility
    - Scan & remediate threats
    - Manage quarantine
    - Install software and database updates
    - Get software info and status
    - Completely remove the software
- Easily deploy to endpoints using an MDM
- Run manually or run using custom automation

System Requirements

Following are minimum requirements for an endpoint on which *Malwarebytes Breach Remediation* may be installed. Please note that these requirements do not include other functionality that the endpoint is responsible for.

- **Operating System:** macOS version 10.12 Sierra or later.
- **Security & Privacy**: Allow apps to be downloaded from Mac App Store and identified developers.
- **Active Internet Connection**: For license validation and protection updates.

External Access Requirements

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

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

Remote Operations

Malwarebytes Breach Remediation can perform its role as a program which is locally installed and operated, or as a program which is remotely deployed and remotely executed. Many system administrators prefer to deploy and operate from a central location, so they can ensure a malware-free working environment and control the methods that are used. The two primary functions covered here are:

- **Deployment –** Installation, registration, and updates of the program on a target endpoint
- **Execution & Remediation –** Scanning the target endpoint for malware threats

Please note that Malwarebytes cannot know which deployment tools that a customer currently uses (if any). For that reason, the required commands are listed here, with the expectation that the customer can supply the appropriate "wrapper" to allow these commands to work in conjunction with their deployment tools.

Using Malwarebytes Breach Remediation

Malwarebytes Breach Remediation is designed specifically for use by IT staff. It may be deployed to an endpoint by local insertion of a USB drive which contains the program, or by pushing the program out to remote endpoints using preferred deployment methods. Once installed on the endpoint, *Malwarebytes Breach Remediation* quickly detects and remediates threats.

PLEASE NOTE: Command line operation is not intended for use by anyone without root access or is not fully familiar with operation of a UNIX operating system.

Manual deployment

Manual deployment requires having access to an admin user account on the target Mac endpoint, and having that account configured to allow remote login (in **System Preferences > Sharing**). In the instructions below, replace **`[adminuser]`** with the username of that admin user and **`[dest_ip]`** with the IP address of that target Mac endpoint.

Deployment

Open **Terminal** on your Mac, then run the following commands:

```
scp /path/to/mbbr-mac.pkg [adminuser]@[dest_ip]:~/
ssh [adminuser]@[dest_ip]
sudo installer -pkg mbbr-mac.pkg -target /
```

Be sure to provide the correct path and installer package name to the mbbr-mac.pkg file on your endpoint in the first command.

Execution

To run *Malwarebytes Breach Remediation* commands on the target Mac, establish a secure shell connection (if you do not still have one open):

```
ssh [adminuser]@[dest_ip]
```

Next, in the secure shell, enter commands like the following (replacing [**`licenseKey`**] with a valid license key):

```
sudo /usr/local/bin/com.malwarebytes.mbbr.tool license activate-key [licenseKey]
sudo /usr/local/bin/com.malwarebytes.mbbr.tool update
sudo /usr/local/bin/com.malwarebytes.mbbr.tool scan
```

Note the use of **`sudo`**; some *Malwarebytes Breach Remediation* commands must be run with root permissions.

Execution

You may use scripts to run *Malwarebytes Breach Remediation* tasks on a recurring basis. To set up a script, log in to the JSS, then go to **Settings > Computer Management > Scripts**. Add a new script. In the Script tab, enter the script you wish to run. For example, to run a diagnostic scan without removing anything, you could use the following shell script (replacing the **`prodKey`** value with a valid key):

```
#!/bin/bash
/usr/local/bin/com.malwarebytes.mbbr.tool license activate-key licenseKey
/usr/local/bin/com.malwarebytes.mbbr.tool update
/usr/local/bin/com.malwarebytes.mbbr.tool scan
```

Please note: It is not strictly necessary to use the **`license`** command every time but doing so will not hurt anything and will ensure the script works in cases where *Malwarebytes Breach Remediation* may never have been registered, or where the registration status may have changed.)

Save this script. Then, add this script to an existing policy, or create a new policy to run the script.

To create a new policy, go to **Computers > Policies** and add a new policy. Add the script to the policy. Set all other options as appropriate for your organization, then save the policy.

The script will now be set to run according to the settings you chose. The policy will run the script with root permissions, which is required by *Malwarebytes Breach Remediation*.

Grant Full Disk Access

IMPORTANT!

Be aware that the scan engine will need to be given Full Disk Access in macOS. If this is not done, it will not be able to detect everything that it should. Full Disk Access (FDA) can be granted manually or via MDM.

To grant FDA manually, go to System Preferences -> Security & Privacy -> Privacy, scroll down and select Full Disk Access, and check the box next to Malwarebytes Protection.app.

Activate License

Getting started with *Malwarebytes Breach Remediation* is very simple. Using an endpoint with a live Internet connection, open the Terminal app and issue the following commands:

```
sudo /usr/local/bin/com.malwarebytes.mbbr.tool license activate-key licenseKey
```

The use of **`sudo`** is not required if your remote admin software gives you root privileges on the target Mac. It is included in this command as a reminder that root privileges are required.

Please note: You must substitute your license key for ***`<licenseKey>`*** in the above example.

Once the program has been activated, it is important to update the app and protection, to ensure you have the latest versions of both. This enables *Malwarebytes Breach Remediation* to detect the latest threats, and ensures the software is fully patched.

Remediation Now or Later?

Malwarebytes Breach Remediation offers the capability to perform a scan only, or to scan and remove detected threats, and will output information about all detections and removals to stdout. This may be valuable in many circumstances, including:

- General assessment of an endpoint's health regarding malware
- Ability to collect and analyze evidence of infections

Scans may be executed for the purpose of remediation, or for diagnostic discovery. A remediation scan combines a scan with a remediation method, so that detected threats may be immediately removed from the endpoint. A diagnostic scan omits the remediation method, so that a scan is executed, and results are reported. The user may then determine how to proceed. This may be valuable if you wish to assess the general health of an endpoint, or if you wish to collect data about one or more endpoints without eliminating evidence that you may wish to retain.

These capabilities are listed below.

Diagnostic Scan

When executing a diagnostic scan, do not provide any specifications for remediation of threats detected during the scan. Detected threats will be output to stdout.

Remediation Scan

A *remediation scan* combines a scan with an automatic remediation method, so that detected threats may be immediately removed from the endpoint. No user intervention is required once the scan begins.

Scan Output

Below is an example of a successful scan:

```
% sudo com.malwarebytes.mbbr.tool scan --detail

Scanning...

Detected Threats:

  Threat Type: malware

       Name: OSX.Genieo

       Path: /Users/test/Library/Application Support/MesCreationsZen2

     Action: quarantined

Scan time: 20.0

Items detected: 1

Items quarantined: 1

Items ignored: 0

Items failed: 0

Some threats that were removed require a restart.
```

Quarantine Output

Below is an example of a successful quarantined object:

% sudo com.malwarebytes.mbbr.tool quarantine list

Quarantine List:

Threat Type: malware

ID: 771BFFE4-4D54-46BA-BA07-D4EDC91547FB

Name: OSX.Genieo

Path: /Users/test/Library/Application Support/MesCreationsZen2

Time (UTC): 2022-02-08 21:47:52 +0000

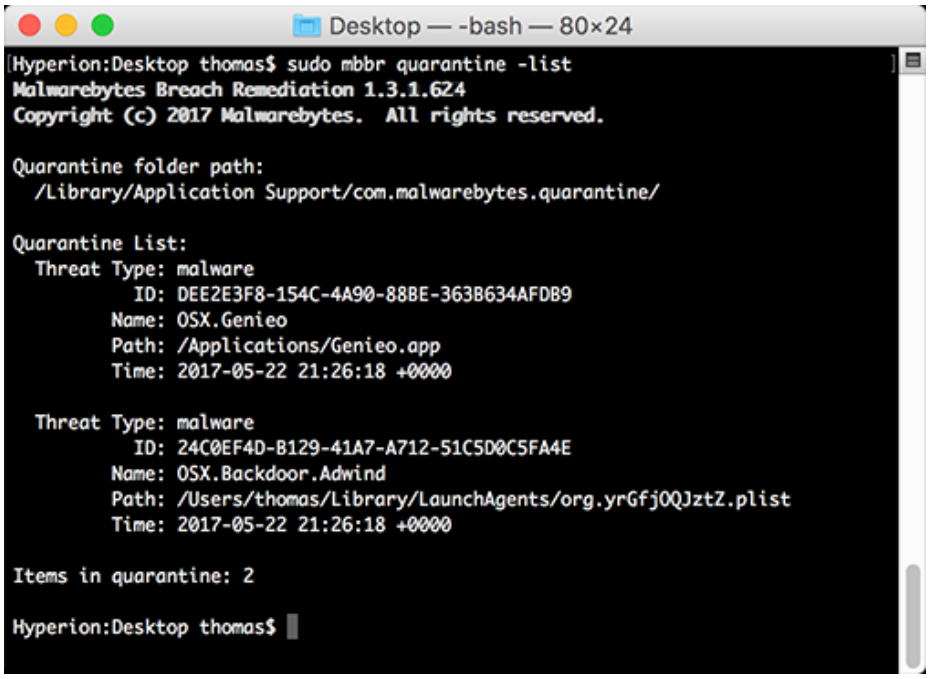
Items in quarantine: 1

Restoring Items from Quarantine

Malwarebytes Breach Remediation offers several different methods of restoring items from quarantine. You may choose either of the following methods:

- **Restore all –** Restores all items currently stored in quarantine to their original locations
- **Restore by id –** This method utilizes quarantine item IDs to selectively restore items to their original locations. This is typically a manual operation, though it may also be performed using a script.

The following screenshot shows a list of items in Quarantine, and how they are represented. The **ID** field is used to specify items to be restored. Please consult page 16 in the Command Line Interface section of this guide for further information.



Command Line Parameters

Malwarebytes Breach Remediation supports a variety of command line parameters, which can be used from a command prompt, batch file, or script. When used from a script, additional commands may be required to support the scripting model being used. Please note: **Root privileges are required for some commands.** Examples will always use *sudo* as a reminder, but *sudo* itself is not required if your remote admin software provides you with the capability to run scripts with root privileges. Using *sudo* with a command that does not require it does not affect the results.

Conventions

The command line structure uses modifiers. These are shown as hyphens (-) immediately preceding parameters. Multiple modifiers may be combined with a parameter. When multiple parameters are used, they must be separated by spaces. In addition, the following conventions are used:

- **text without brackets or braces**
  Items you must type as shown
- **<text inside angle brackets>**
  Required information for which you must supply a value
  Example: **sudo mbbr <*parameter_1*>**
- **[text inside square brackets]**
  Optional items
  Example: **sudo mbbr [*parameter_1*]**
- **Grouping of dots (…)**
  A set of specifications
  Example: **sudo mbbr <*parameter _1*> [*parameter_2*] … [*parameter_n*]**
- **{text inside braces}**
  A set of required items; choose one from the list provided
  Example: **sudo mbbr {0 | 1 | 2 | 3}**
- **vertical bar (|)**
  Separator between mutually exclusive items; choose one
  Example: **sudo mbbr <0 | 1 | 2 | 3>**

Command Line Overview

Following is a list of high-level commands which may be executed. Each command is detailed beginning on the next page.

version	Displays the program version number.
license	Manage your license.
scan	Scans the endpoint for malware and optionally removes malware found during the scan.
status	Displays the status of the application.
update	Downloads the most recent protection updates.
quarantine	Controls program actions related to threat quarantine activities.
uninstall	Uninstalls the program from the endpoint.

To see usage information for one specific command, use the **–h** or **--help**. For example, to get usage information for the scan command, the following command can be used:

```
sudo com.malwarebytes.mbbr.tool scan --help
```

Command Line Reference

Commands listed here are listed individually. Each command performs tasks according to parameters. These are primarily used by a system administrator via script, batch file, GPO update, or remote desktop. The admin may configure *Malwarebytes Breach Remediation* to operate as a remote task, invisible to the endpoint user.

version

Usage:

sudo com.malwarebytes.mbbr.tool version

Purpose:

Displays the version number of Malwarebytes Breach Remediation.

Parameters:

None

license

Usage:

sudo com.malwarebytes.mbbr.tool license

[activate-key]

[deactivate]

[state]

Purpose:

Display and manage your Malwarebytes Breach Remediation license information based on the parameters specified.

Parameters:

activate-key

Activates license key.

deactivate

Deactivates license key.

state

Displays license key state.

scan

Usage:

sudo com.malwarebytes.mbbr.tool scan

[--ignore-pup]

{ [--remove] | [--no-remove] }

{ [--reboot] | [--no-reboot] }

{ [--no-output] | [--summary] | [--detail] }

Purpose:

Executes a scan based on parameters specified. Requires root privileges.

Parameters:

--ignore-pup

Instructs the scanner to ignore all Potentially Unwanted Programs PUPs that may be installed on the target endpoint.

--remove

Instructs the scanner to quarantine any malware, adware and PUPs found during the scan. (This is the default if neither --remove or --no-remove is included.)

--no-remove

Instructs the scanner to not quarantine detected malware, adware, and PUPs found during the scan.

--reboot

Some malware executes in a manner that requires a reboot to complete the removal process. If this occurs, the scanner will automatically reboot the system.

-noreboot

If an immediate reboot on removal is not desired, use this option. Please note that certain malware may not be fully removed if this option is used. (This is the default if neither --reboot or --noreboot is included.)

--no-output | --detail | --summary

Controls the level of output to the console. Defaults to **summary** if not specified. For full information about threats removed, use **detail**.

status

Usage:

sudo com.malwarebytes.mbbr.tool status

[--license]

[--permissions]

[--reboot]

Purpose:

Display status of Malwarebytes Breach Remediation.

Parameters:

--license

Displays license key status.

--permissions

Alerts if Full Disk Access has not been granted. (See Remote Operations section for details.)

--reboot

Alerts if malware was previously removed that required a reboot, but the machine has not yet been rebooted.

update

Usage:

sudo com.malwarebytes.mbbr.tool update

[--database] { [check] | [config] | [install] }

[--engine] { [check] | [config] | [install] }

Purpose:

Manage protection database and software engine updates. Used without any options, this command will download and install any needed updates, for both the engine and the database. Use the options for more fine-grained control

Parameters:

--database

Download protection database updates.

--reboot

Download software engine updates.

check

Checks for program available database and/or engine updates.

config

Manages configuration of updates, such as whether to install early access (beta) engine updates. For more info, see *com.malwarebytes.mbbr.tool update config --help*

install

Installs available database and/or engine updates.

quarantine

Usage:

sudo com.malwarebytes.mbbr.tool quarantine

[list]

[delete] [--al]

[restore] [--all]

Purpose:

List contents, delete, and restore items from the quarantine.

Parameters:

list

Shows the current quarantine location and lists contents of the quarantine to screen output. Output includes an ID for each item in the database, for use with other options.

restore: --all | <UUID1>[,<UUID2>…,<UUIDn>]

Restores one or more items from the list of quarantined items. Items are specified by their ID. When multiple items are to be restored via a single execution of this command, their IDs should be separated by commas without delimiting spaces. Use of the --all option restores all items in the quarantine database.

delete: --all | <UUID1>[,<UUID2>…,<UUIDn>]

Deletes one or more items from the list of quarantined items. Items are specified by their ID. When multiple items are restored using a single execution of this command, their IDs should

be separated by commas without delimiting spaces. Use of the --all option deletes all items in the quarantine database.

uninstall

Usage:

sudo com.malwarebytes.mbbr.tool uninstall

Purpose:

Completely removes the software from the endpoint. Requires root privileges on the endpoint.

Parameters:

None