Malwarebytes | TOOLSET

Toolset
User Guide

22 March 2024

Notices

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

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

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

Third Party Project Usage

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

https://support.malwarebytes.com/hc/en-us/articles/360038649894

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

Table of Contents (continued)

Table of Contents (continued)

Introduction

Welcome to the *Malwarebytes Toolset*!! – a collection of tools developed for technicians by technicians. This toolset will help drive efficient processes and procedures in malware remediation and computer repair, ensuring technicians have the right tools at the right time to get the job done.

Malwarebytes Toolset provides the following primary components:

- **Inform –** Quick access to essential diagnostic/triage information about the PC and local network
    - **Network Devices Scanner –** Quickly discover local network devices like routers, printers, computers, media streaming devices and more.
- **Scan –** An automated wizard that helps remediate malware, resolve OS issues, and discover failing hardware
    - **Malwarebytes Portable Scanner –** Customizable malware scanning of the computer
    - **Issue Scanner –** Inspection of the operating system, system logs, disk drives, devices and connectivity.
- **Toolbox –** A one stop-shop for additional standalone tools and OS utilities
    - **MyTools –** Integrate your own tools in to the Toolbox to fit your specific needs
    - **Malwarebytes Technician Tools –** Access to additional Malwarebytes Tools like AdwCleaner, Anti-Rootkit, Anti-Bundleware and command line-based malware/rootkit scanning
    - ***Malwarebytes Installer* –** Access to easily install the consumer version of *Malwarebytes for Windows* and related web browser extensions on your client's PCs to get them protected from modern malware threats

Your clients depend on you and your skills while you depend on your tools and in-depth experience to save the day. *Malwarebytes Toolset* ensures that you can meet those goals by having the right tools at the right time to get the job done.

System Requirements

Following are minimum requirements for a computer system on which *Malwarebytes Toolset* may be installed. Please note that these requirements do not include any other functionality that the computer is responsible for.

- **Operating System:** Windows 10, Windows 8.1, Windows 8, and Windows 7
- **Application Framework:** .NET Framework 4.5
- **CPU:** 1 GHz or faster with SSE2 technology. This technology is used in most modern Intel x86 processors as well as AMD's Athlon 64, Sempron 64, Turion 64 and Phenom CPU families. For further information about SSE2, please go to:

    https://en.wikipedia.org/wiki/SSE2

- **RAM:** 2 GB (64-bit OS), 1 GB (32-bit OS)
- **Free Disk Space:** 150 MB
- **Recommended Screen Resolution:** 1024x768 or higher, 1336x768 recommended
- **Active Internet Connection**
- **Network Discovery/SSDP Discovery Service Enabled** (required for Network Devices scanner)

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 Toolset* to reach Malwarebytes services. These are:

https://toolset.malwarebytes.com	Port 443	outbound
https://telemetry.malwarebytes.com	Port 443	outbound
https://data.service.malwarebytes.com	Port 443	outbound
https://data-cdn.mbamupdates.com	Port 443	outbound
https://data-cdn-static.mbamupdates.com	Port 443	outbound

https://hubble.mb-cosmos.com	Port 443	outbound
https://blitz.mb-cosmos.com	Port 443	outbound
https://*.mwbsys.com	Port 443	outbound

Program Licensing

A valid license is required to use the *Malwarebytes Toolset*. Validation requires Internet access and is valid for fifteen (15) days of offline use. Each time *Malwarebytes Toolset* is launched, a silent revalidation will occur. Should the license become expired, blocked, or deleted, an error will be displayed, and the user will be given an opportunity to reenter the license. You can also manage your license key in the Settings component of the *Malwarebytes Toolset*. If you need further assistance with your license, contact techbench@malwarebytes.com.

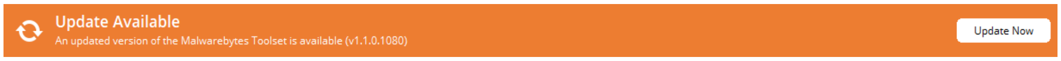
First Time Use

When you first use the *Malwarebytes Toolset*, you will need internet access to allow it to validate your license key and to update the toolset components.

1. Download the *Malwarebytes Toolset* with your license key pre-injected using the URL contained in your confirmation email.
2. Extract the MBTS_X.X.X.XXXX.zip package file to the root of a USB flash drive or a dedicated directory within a USB Flash Drive.
    - Note: Ensure the path where *Malwarebytes Toolset* is extracted to does not include any ASCII/UNICODE extended set characters.
3. Double click **MBTSLauncher.exe** from the extracted package.
4. Once the *Malwarebytes Toolset* has launched and validated your license, go to **Toolbox** ► **MyTools** ► **Check for Updates**
5. Download all available updates

Staying Up to Date

Upon launching *Malwarebytes Toolset*, a silent check for an update is performed. If one is available, an orange Update Available notification bar will appear below the black menu bar. Click **Update Now** to see what updates are available. Initiate the update process and follow the additional prompts.



Update Available

An updated version of the Malwarebytes Toolset is available (v1.1.0.1080)

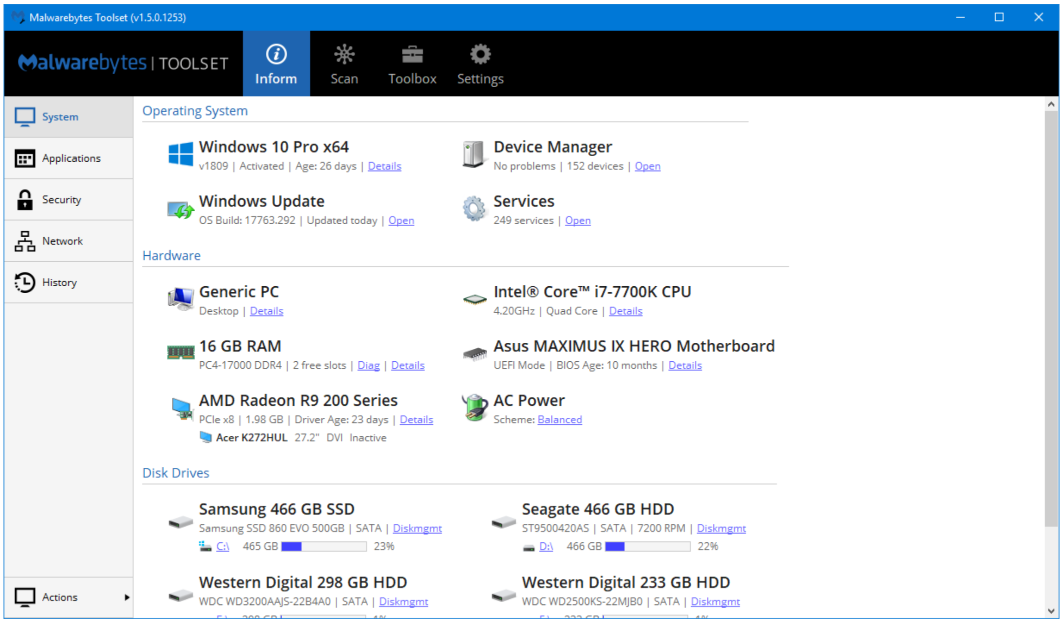
For all other components, or to manually update, use the **Check for Updates Tool** by doing the following (recommended daily):

1. Launch *Malwarebytes Toolset.*
2. Click on the Toolbox component.
3. Go to **MyTools** and click **Check for Updates**
4. Select the components you want to update, then click **Download**
5. Follow any additional steps presented.

We will always check for the latest version of a tool before it is launched from the Toolbox. If a new version is available, we give you the option to download it or to continue using the version already on the Toolset.

Screen Layout

The *Malwarebytes Toolset* user interface is divided into three sections, as shown below.



Operating System

Windows 10 Pro x64
v1809 | Activated | Age: 26 days | Details

Device Manager
No problems | 152 devices | Open

Windows Update
OS Build: 17763.292 | Updated today | Open

Services
249 services | Open

Hardware

Generic PC
Desktop | Details

Intel® Core™ i7-7700K CPU
4.20GHz | Quad Core | Details

16 GB RAM
PC4-17000 DDR4 | 2 free slots | Diag | Details

Asus MAXIMUS IX HERO Motherboard
UEFI Mode | BIOS Age: 10 months | Details

AMD Radeon R9 200 Series
PCIe x8 | 1.98 GB | Driver Age: 23 days | Details
Acer K272HUL 27.2" DVI Inactive

AC Power
Scheme: Balanced

Disk Drives

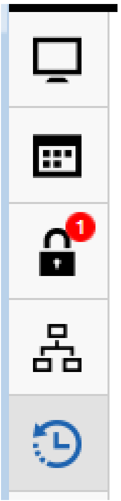
Samsung 466 GB SSD
Samsung SSD 860 EVO 500GB | SATA | Diskmgmt
C:\ 465 GB 23%

Seagate 466 GB HDD
ST9500420AS | SATA | 7200 RPM | Diskmgmt
D:\ 466 GB 22%

Western Digital 298 GB HDD
WDC WD3200AAJS-22B4A0 | SATA | Diskmgmt

Western Digital 233 GB HDD
WDC WD2500KS-22MJB0 | SATA | Diskmgmt

The Mode selector is shown across the top, in the black area. The Option selector is displayed vertically, at the left edge of the screen. It is present only in Inform mode. The majority of the screen is reserved for system information related to the selected option. When in Scan mode or Toolbox, the area used for the Option selector is allocated for use by the program as a whole.



The interface size may be increased or decreased at will. The names of the options will disappear when the interface size decreases beyond a certain point, leaving only the icons showing.

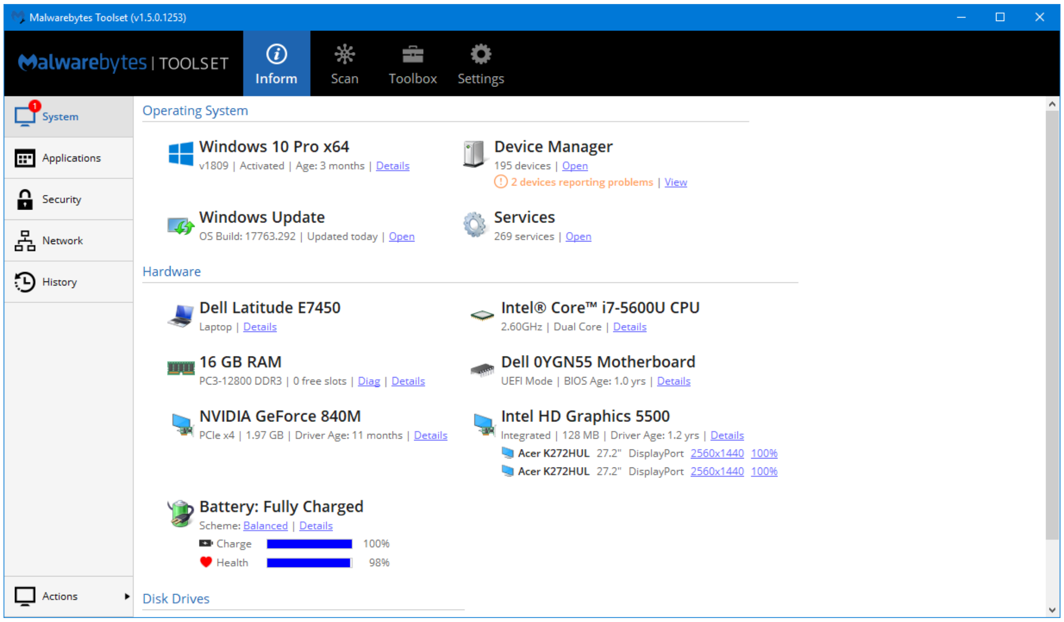
As you can see, the Security option (the padlock) contains a warning to alert the user to a security-related situation which should be investigated.

Inform

This program mode is designed to tell you about the state of your system. You may encounter issues related to hardware, software or malware. Before attempting to diagnose any failure, it is best to gather information. Five options are available to you here, to provide that information in an organized manner. **Please note** that icons for each item are obtained from the operating system that *Malwarebytes Toolset* is installed on. As a result, the specific icons shown are system-dependent. Let's look at this program mode in detail.

System tab

The System tab offers basic information about a computer. When servicing a computer which has issues, the first thing a technician must do is to know what they are working with. Important characteristics of the computer will be shown here. Problems may be visible on this screen, though deeper investigation will likely be required. Please refer to the screenshot shown below.



Operating System

Windows 10 Pro x64
v1809 | Activated | Age: 3 months | Details

Device Manager
195 devices | Open
2 devices reporting problems | View

Windows Update
OS Build: 17763.292 | Updated today | Open

Services
269 services | Open

Hardware

Dell Latitude E7450
Laptop | Details

Intel® Core™ i7-5600U CPU
2.60GHz | Dual Core | Details

16 GB RAM
PC3-12800 DDR3 | 0 free slots | Diag | Details

Dell 0YGN55 Motherboard
UEFI Mode | BIOS Age: 1.0 yrs | Details

NVIDIA GeForce 840M
PCIe x4 | 1.97 GB | Driver Age: 11 months | Details

Intel HD Graphics 5500
Integrated | 128 MB | Driver Age: 1.2 yrs | Details
Acer K272HUL 27.2" DisplayPort 2560x1440 100%
Acer K272HUL 27.2" DisplayPort 2560x1440 100%

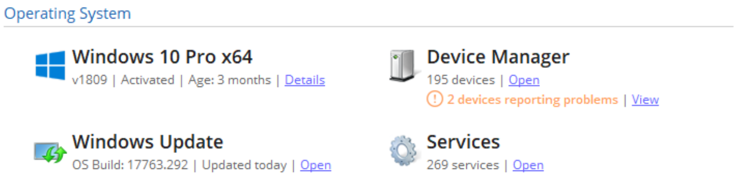
Battery: Fully Charged
Scheme: Balanced | Details
Charge 100%
Health 98%

Disk Drives

While a wealth of information is available to the technician on this screen, tools designed specifically for the purpose of evaluating issues on the computer will be discussed later. Many of the topics shown here have a clickable Details link, allowing you to find out more. When viewing those details, you may right click any individual detail to copy its value into your clipboard for use elsewhere.

Operating System

Here, you can find information pertaining to your operating system installation, Services and Device Manager. **Services** and **Device Manager** both launch function-specific snap-ins of the Microsoft Management Console. You can also inspect or perform Windows updates, as well as change update settings.



Operating System

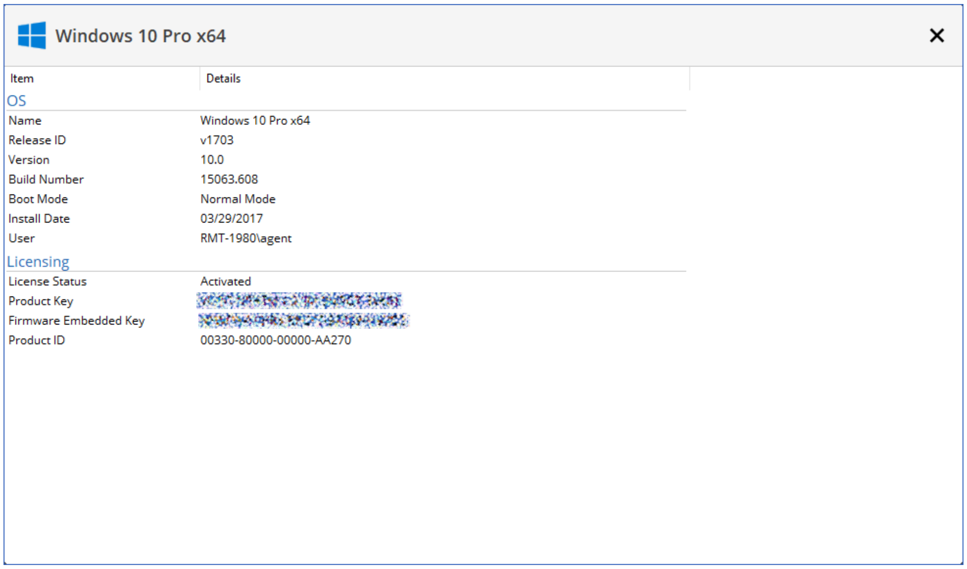
Windows 10 Pro x64
v1809 | Activated | Age: 3 months | Details

Device Manager
195 devices | Open
2 devices reporting problems | View

Windows Update
OS Build: 17763.292 | Updated today | Open

Services
269 services | Open

Please note that the Operating System Details displays the Product Key (license) associated with the operating system installation, as well as the Firmware Embedded Key (a Windows license key that may be embedded in firmware by motherboard vendors or by Microsoft for Digital Entitlement). In most cases, this information is unique to the OS installation and should not be shared.

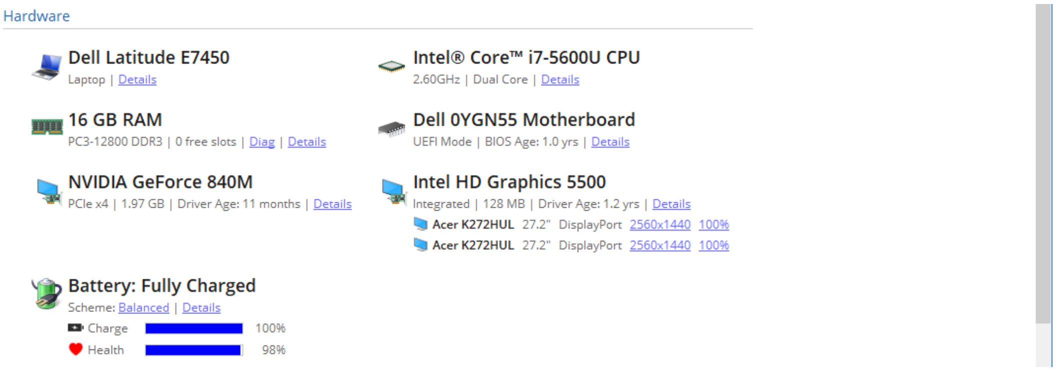


Windows 10 Pro x64

Item	Details
OS	
Name	Windows 10 Pro x64
Release ID	v1703
Version	10.0
Build Number	15063.608
Boot Mode	Normal Mode
Install Date	03/29/2017
User	RMT-1980\agent
Licensing	
License Status	Activated
Product Key	[redacted]
Firmware Embedded Key	[redacted]
Product ID	00330-80000-00000-AA270

Hardware

Each major system component is itemized here. Feel free to click any **Details** link to find out more. Windows settings for some hardware devices can also be changed here. On portable devices, detailed battery charge and health information is displayed.



Hardware

Dell Latitude E7450
Laptop | Details

Intel® Core™ i7-5600U CPU
2.60GHz | Dual Core | Details

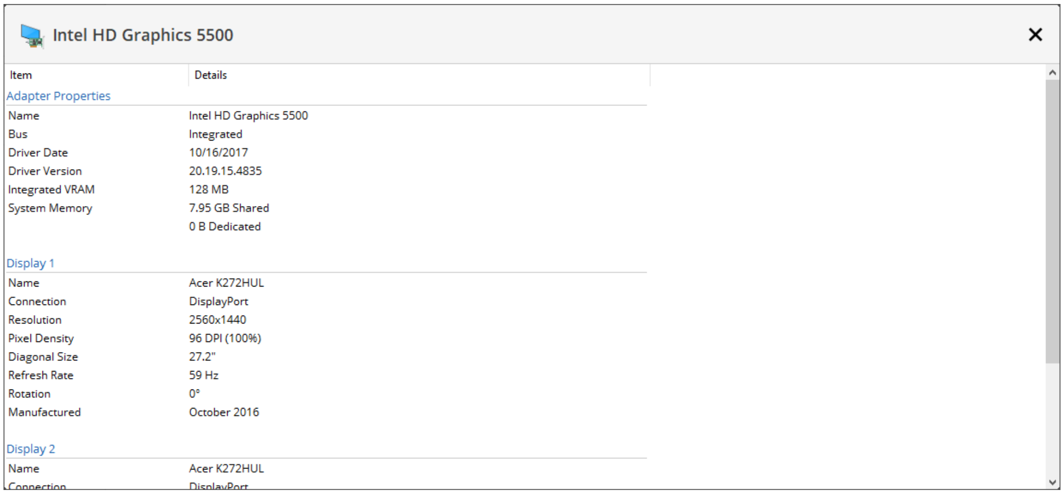
16 GB RAM
PC3-12800 DDR3 | 0 free slots | Diag | Details

Dell 0YGN55 Motherboard
UEFI Mode | BIOS Age: 1.0 yrs | Details

NVIDIA GeForce 840M
PCIe x4 | 1.97 GB | Driver Age: 11 months | Details

Intel HD Graphics 5500
Integrated | 128 MB | Driver Age: 1.2 yrs | Details
Acer K272HUL 27.2" DisplayPort 2560x1440 100%
Acer K272HUL 27.2" DisplayPort 2560x1440 100%

Battery: Fully Charged
Scheme: Balanced | Details
Charge 100%
Health 98%

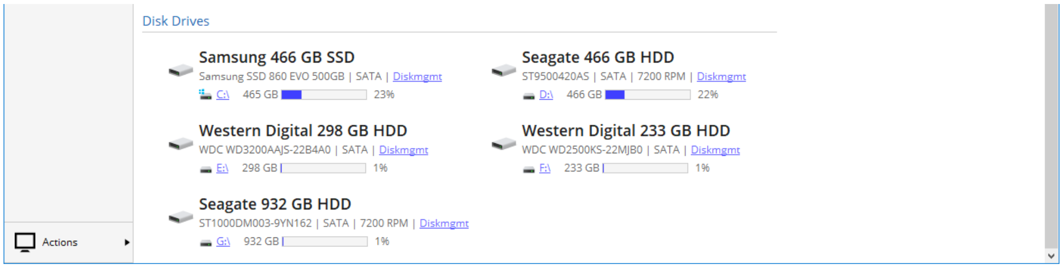


Intel HD Graphics 5500

Item	Details
Adapter Properties	
Name	Intel HD Graphics 5500
Bus	Integrated
Driver Date	10/16/2017
Driver Version	20.19.15.4835
Integrated VRAM	128 MB
System Memory	7.95 GB Shared 0 B Dedicated
Display 1	
Name	Acer K272HUL
Connection	DisplayPort
Resolution	2560x1440
Pixel Density	96 DPI (100%)
Diagonal Size	27.2"
Refresh Rate	59 Hz
Rotation	0°
Manufactured	October 2016
Display 2	
Name	Acer K272HUL
Connection	DisplayPort

Disk Drives

Information for each disk drive installed in the computer can be viewed here as well. **Diskmgmt** links provide access to the Microsoft Management Console snap-in, allowing inspection and/or modification of disk partitions. The drive letter associated with each disk drive is also a clickable link, providing access to File Explorer/Windows Explorer (application name dependent on operating system version in use).



Disk Drives

Samsung 466 GB SSD
Samsung SSD 860 EVO 500GB | SATA | Diskmgmt
C:\ 465 GB 23%

Seagate 466 GB HDD
ST9500420AS | SATA | 7200 RPM | Diskmgmt
D:\ 466 GB 22%

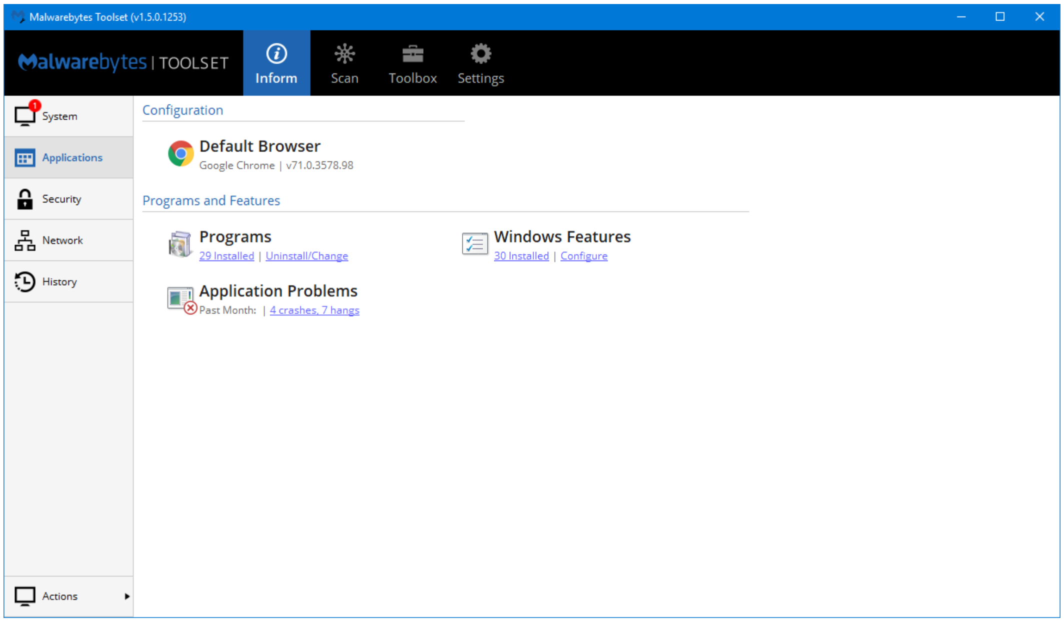
Western Digital 298 GB HDD
WDC WD3200AAJS-22B4A0 | SATA | Diskmgmt
E:\ 298 GB 1%

Western Digital 233 GB HDD
WDC WD2500KS-22MJB0 | SATA | Diskmgmt
F:\ 233 GB 1%

Seagate 932 GB HDD
ST1000DM003-9YN162 | SATA | 7200 RPM | Diskmgmt
G:\ 932 GB 1%

Applications tab

This tab is focused on software installed on the target computer, and on system settings which control operation of programs. These settings are commonly used by malware to modify system operation, further enabling operation of the malware.



Malwarebytes Toolset (v1.5.0.1253)

Configuration

Default Browser
Google Chrome | v71.0.3578.98

Programs and Features

Programs
29 Installed | Uninstall/Change

Windows Features
30 Installed | Configure

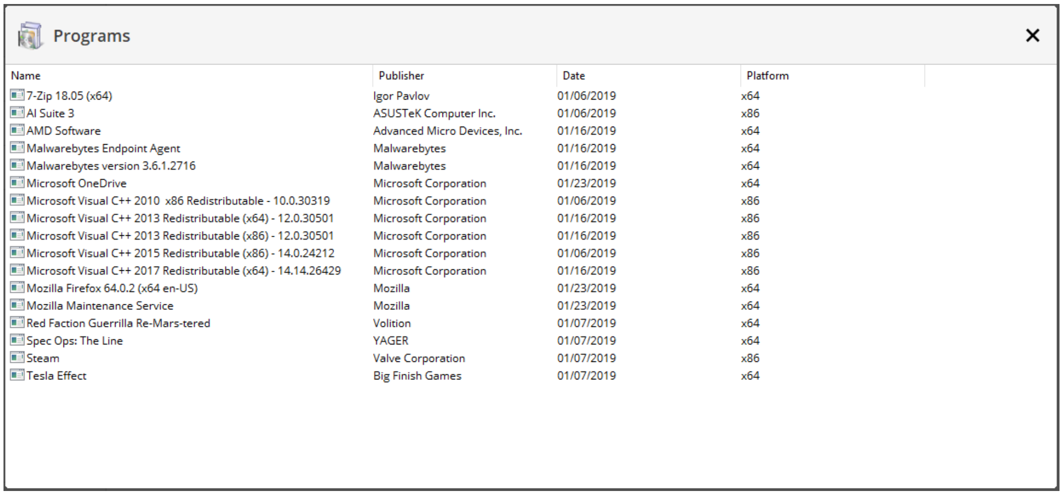
Application Problems
Past Month: | 4 crashes, 7 hangs

Configuration

Default Browser is not symptomatic of any kind of system problem. Instead, it helps the technician ascertain the characteristics of the user. That, combined with many other factors, may influence troubleshooting methods.

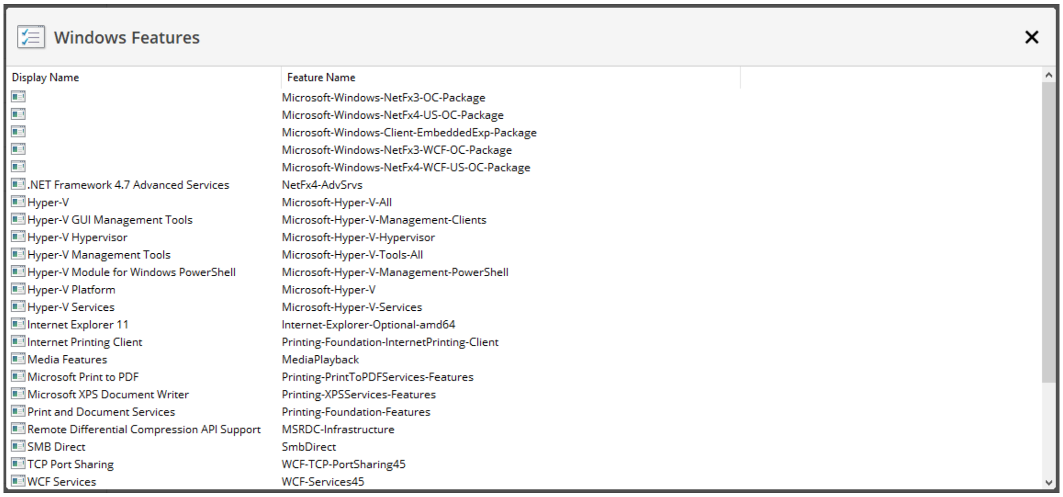
Programs and Features

Programs relate to desktop applications installed on the computer, as well as some system add-on components and drivers. Clicking the link that states the number of installed programs will open a window that lists detected installed applications. This detailed list includes Name, Publisher, Date of installation, and Platform (e.g. x86, x64, etc). Clicking **Uninstall/Change** will launch the Programs and Features component of the Windows Control Panel.



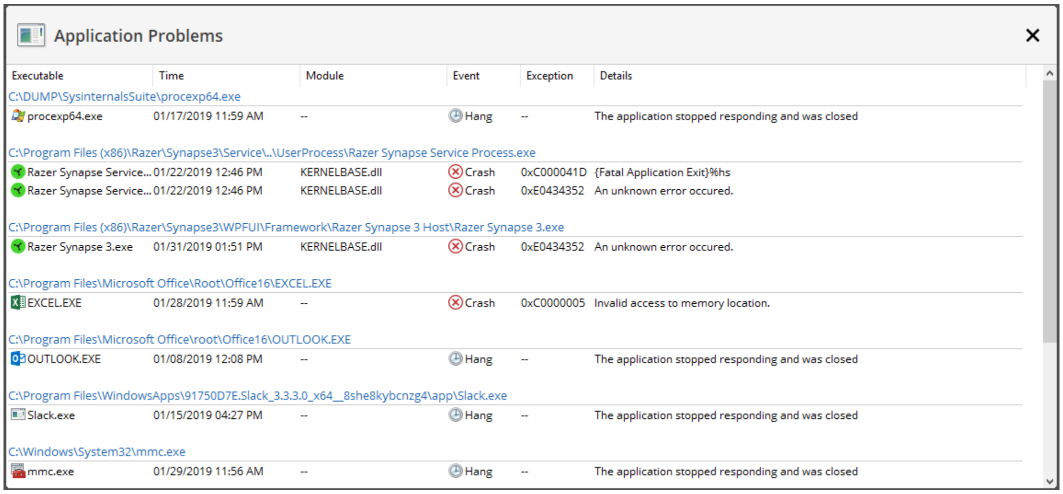
Name	Publisher	Date	Platform
7-Zip 18.05 (x64)	Igor Pavlov	01/06/2019	x64
AI Suite 3	ASUSTeK Computer Inc.	01/06/2019	x86
AMD Software	Advanced Micro Devices, Inc.	01/16/2019	x64
Malwarebytes Endpoint Agent	Malwarebytes	01/16/2019	x64
Malwarebytes version 3.6.1.2716	Malwarebytes	01/16/2019	x64
Microsoft OneDrive	Microsoft Corporation	01/23/2019	x64
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319	Microsoft Corporation	01/06/2019	x86
Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501	Microsoft Corporation	01/16/2019	x86
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501	Microsoft Corporation	01/16/2019	x86
Microsoft Visual C++ 2015 Redistributable (x86) - 14.0.24212	Microsoft Corporation	01/06/2019	x86
Microsoft Visual C++ 2017 Redistributable (x64) - 14.14.26429	Microsoft Corporation	01/16/2019	x86
Mozilla Firefox 64.0.2 (x64 en-US)	Mozilla	01/23/2019	x64
Mozilla Maintenance Service	Mozilla	01/23/2019	x64
Red Faction Guerrilla Re-Mars-tered	Volition	01/07/2019	x64
Spec Ops: The Line	YAGER	01/07/2019	x64
Steam	Valve Corporation	01/07/2019	x86
Tesla Effect	Big Finish Games	01/07/2019	x64

Windows Features are optional capabilities which are beyond the scope of normal operating system functionality. Clicking the link that states the number of installed features will open a window with information on the currently installed features. This list includes Display Name and Feature Name. Clicking **Configure** will launch the Windows Feature component of Control Panel.



Display Name	Feature Name
	Microsoft-Windows-NetFx3-OC-Package
	Microsoft-Windows-NetFx4-US-OC-Package
	Microsoft-Windows-Client-EmbeddedExp-Package
	Microsoft-Windows-NetFx3-WCF-OC-Package
	Microsoft-Windows-NetFx4-WCF-US-OC-Package
.NET Framework 4.7 Advanced Services	NetFx4-AdvSrvs
Hyper-V	Microsoft-Hyper-V-All
Hyper-V GUI Management Tools	Microsoft-Hyper-V-Management-Clients
Hyper-V Hypervisor	Microsoft-Hyper-V-Hypervisor
Hyper-V Management Tools	Microsoft-Hyper-V-Tools-All
Hyper-V Module for Windows PowerShell	Microsoft-Hyper-V-Management-PowerShell
Hyper-V Platform	Microsoft-Hyper-V
Hyper-V Services	Microsoft-Hyper-V-Services
Internet Explorer 11	Internet-Explorer-Optional-amd64
Internet Printing Client	Printing-Foundation-InternetPrinting-Client
Media Features	MediaPlayback
Microsoft Print to PDF	Printing-PrintToPDFServices-Features
Microsoft XPS Document Writer	Printing-XPSServices-Features
Print and Document Services	Printing-Foundation-Features
Remote Differential Compression API Support	MSRDC-Infrastructure
SMB Direct	SmbDirect
TCP Port Sharing	WCF-TCP-PortSharing45
WCF Services	WCF-Services45

Application Problems gives insight on applications that have crashed or hung on the system. Clicking the link that states the number of crashes/hangs will open a list of the detected problems. The list is grouped by the problem process and includes the Executable that failed, Time of failure, Module that failed, Event type, Exception code, and detailed error message.

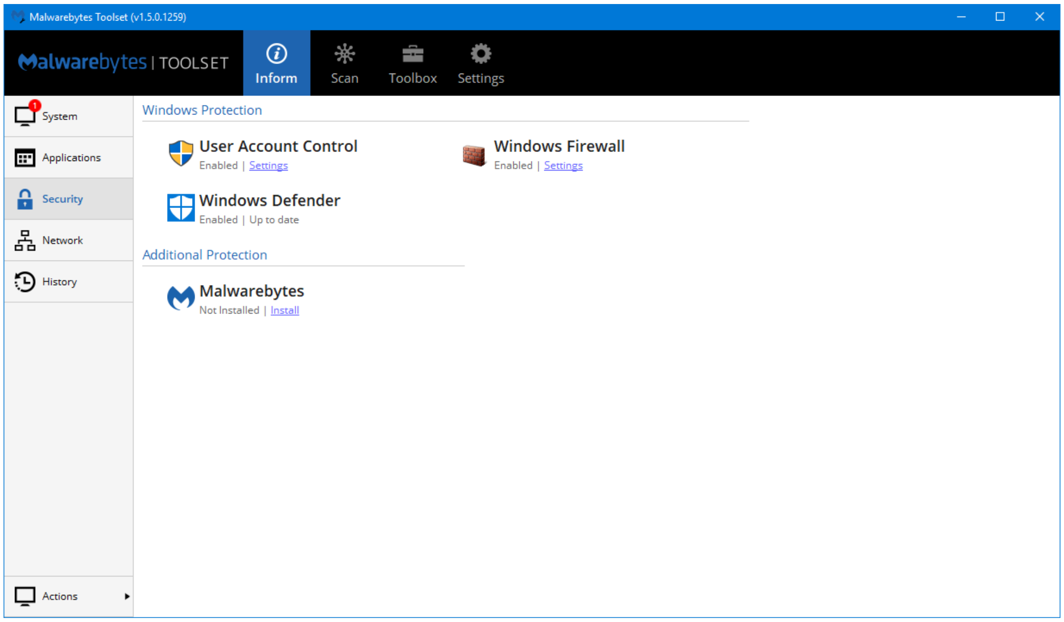


Application Problems

Executable	Time	Module	Event	Exception	Details
C:\DUMP\SysinternalsSuite\procexp64.exe					
procexp64.exe	01/17/2019 11:59 AM	--	Hang	--	The application stopped responding and was closed
C:\Program Files (x86)\Razer\Synapse3\Service\..\UserProcess\Razer Synapse Service Process.exe					
Razer Synapse Service...	01/22/2019 12:46 PM	KERNELBASE.dll	Crash	0xC000041D	{Fatal Application Exit}%hs
Razer Synapse Service...	01/22/2019 12:46 PM	KERNELBASE.dll	Crash	0xE0434352	An unknown error occured.
C:\Program Files (x86)\Razer\Synapse3\WPFUI\Framework\Razer Synapse 3 Host\Razer Synapse 3.exe					
Razer Synapse 3.exe	01/31/2019 01:51 PM	KERNELBASE.dll	Crash	0xE0434352	An unknown error occured.
C:\Program Files\Microsoft Office\Root\Office16\EXCEL.EXE					
EXCEL.EXE	01/28/2019 11:59 AM	--	Crash	0xC0000005	Invalid access to memory location.
C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE					
OUTLOOK.EXE	01/08/2019 12:08 PM	--	Hang	--	The application stopped responding and was closed
C:\Program Files\WindowsApps\91750D7E.Slack_3.3.3.0_x64__8she8kybcnzg4\app\Slack.exe					
Slack.exe	01/15/2019 04:27 PM	--	Hang	--	The application stopped responding and was closed
C:\Windows\System32\mmc.exe					
mmc.exe	01/29/2019 11:56 AM	--	Hang	--	The application stopped responding and was closed

Security tab

This tab controls security features of the computer, both built-in and add-on. It is primarily designed as a quick verification of security practices being used on the computer.



Malwarebytes Toolset (v1.5.0.1259)

Windows Protection

User Account Control
Enabled | Settings

Windows Firewall
Enabled | Settings

Windows Defender
Enabled | Up to date

Additional Protection

Malwarebytes
Not Installed | Install

Windows Protection

These items pertain to security features built into Windows operating systems. A brief description of each protection item is as follows:

- **User Account Control** (UAC) – which made its debut as part of Windows Vista – requests your authorization before allowing programs to perform an operation that may affect computer operations or change performance characteristics. If your computer is not under the control of a system administrator, you may alter UAC settings.
- **Windows Firewall** controls access to your computer, with default settings specified for each profile (domain, private, public). In addition to default settings, you may specify unique new firewall rules, and modify or delete existing rules.

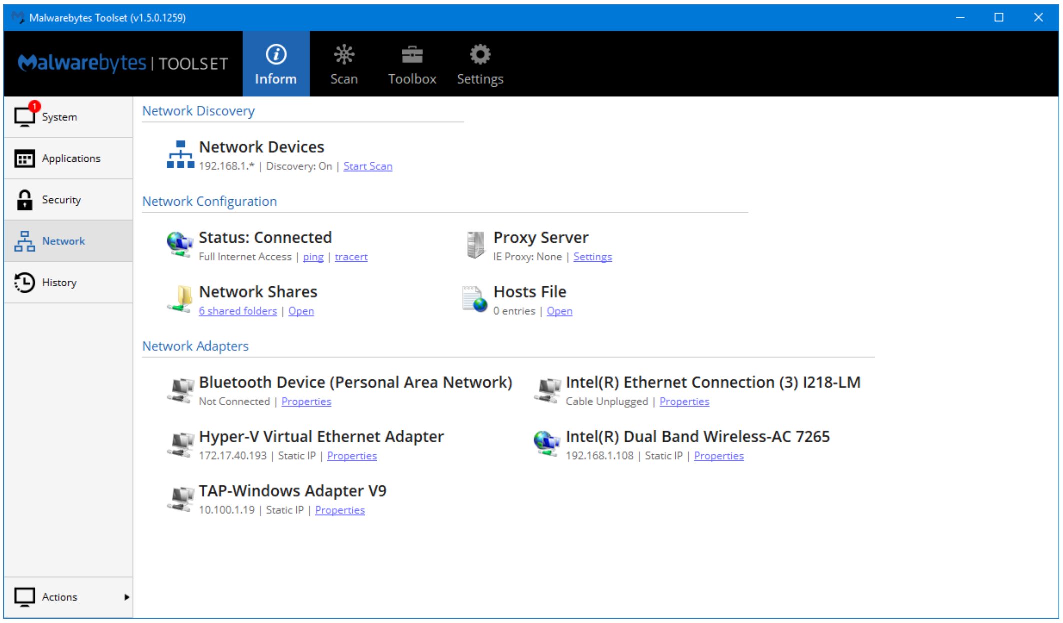
- **Windows Defender** is an antivirus program offered by Microsoft on computers using Windows 8 (and newer) operating systems. Windows Defender was not classified as an antivirus program prior to Windows 8, therefore it would not be listed for earlier operating systems.

Additional Protection

This tab provides information about additional security applications (Malwarebytes and other antivirus/antimalware applications) installed on the computer. These applications are in addition to those provided by the operating system. There are no provisions to change settings associated with these external programs. If no antivirus software is installed, a link to install Malwarebytes will be shown.

Network tab

This tab provides information about your networking environment. Any networking-related issues noted during the system scan will be shown here as well. A screenshot of this tab is below.



Network Discovery

Network Devices
192.168.1.* | Discovery: On | Start Scan

Network Configuration

Status: Connected
Full Internet Access | ping | tracert

Proxy Server
IE Proxy: None | Settings

Network Shares
6 shared folders | Open

Hosts File
0 entries | Open

Network Adapters

Bluetooth Device (Personal Area Network)
Not Connected | Properties

Intel(R) Ethernet Connection (3) I218-LM
Cable Unplugged | Properties

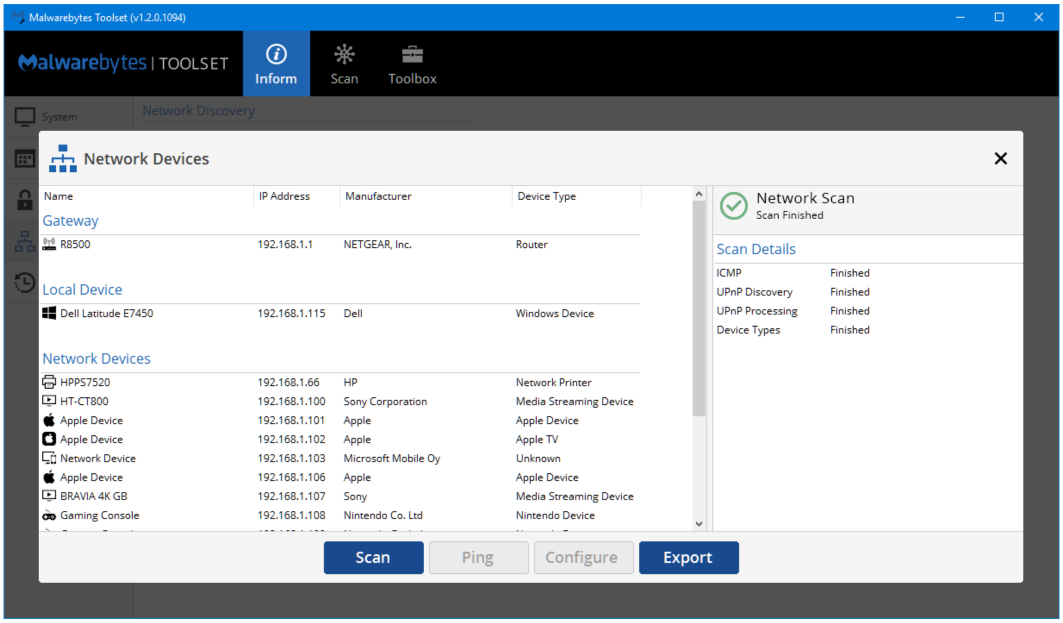
Hyper-V Virtual Ethernet Adapter
172.17.40.193 | Static IP | Properties

Intel(R) Dual Band Wireless-AC 7265
192.168.1.108 | Static IP | Properties

TAP-Windows Adapter V9
10.100.1.19 | Static IP | Properties

Network Discovery & Network Devices Scanner

This section provides access to the Network Devices scanner to quickly discover local network devices like routers, printers, computers, media streaming devices, mobile devices, game consoles, and more. The tile will list the current IP scheme of the local network, the current state of the Network Discovery Service (required for the Network Devices scanner), and a link to open the Network Devices scanner window. Click **Start Scan** to launch the Network Devices window and begin scanning the local network for devices as shown below. Scan status is shown on the right side.



Name	IP Address	Manufacturer	Device Type
Gateway			
R8500	192.168.1.1	NETGEAR, Inc.	Router
Local Device			
Dell Latitude E7450	192.168.1.115	Dell	Windows Device
Network Devices			
HPPS7520	192.168.1.66	HP	Network Printer
HT-CT800	192.168.1.100	Sony Corporation	Media Streaming Device
Apple Device	192.168.1.101	Apple	Apple Device
Apple Device	192.168.1.102	Apple	Apple TV
Network Device	192.168.1.103	Microsoft Mobile Oy	Unknown
Apple Device	192.168.1.106	Apple	Apple Device
BRAVIA 4K GB	192.168.1.107	Sony	Media Streaming Device
Gaming Console	192.168.1.108	Nintendo Co. Ltd	Nintendo Device

Network Scan
Scan Finished

Scan Details

ICMP	Finished
UPnP Discovery	Finished
UPnP Processing	Finished
Device Types	Finished

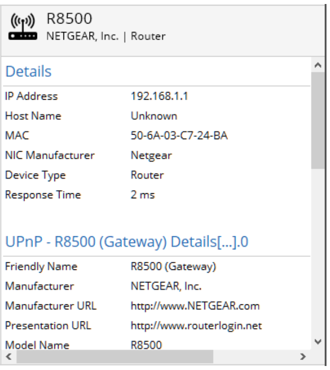
The Network Devices scan uses the following methods:

- ICMP/PING
- ARP Cache
- DNS Resolution
- Universal Plug and Play (UPnP)
- Simple Service Discovery Protocol (SSDP)
- Web Services on Devices (WSD)
- Windows Connect Now (WCN)
- Selected Port/Service scanning

Devices are sorted by IP address into three categories:

- Gateway – the network device–usually a router or access point–that is serving you network and internet access.
- Local Device – the device you are currently running the Network Devices scanner from
- Network Devices – Other network devices connected to the same network as the Local Device

The following screenshots show typical data for each of the three network device categories (after one of them has been selected). Please note that Plug and Play information is shown for devices which support this feature.



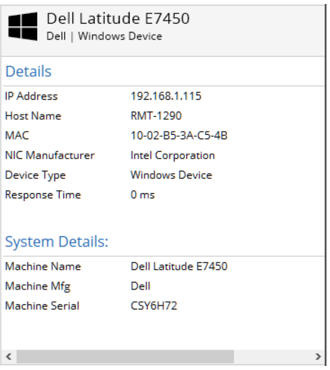
R8500
NETGEAR, Inc. | Router

Details

IP Address	192.168.1.1
Host Name	Unknown
MAC	50-6A-03-C7-24-BA
NIC Manufacturer	Netgear
Device Type	Router
Response Time	2 ms

UPnP - R8500 (Gateway) Details[...].0

Friendly Name	R8500 (Gateway)
Manufacturer	NETGEAR, Inc.
Manufacturer URL	http://www.NETGEAR.com
Presentation URL	http://www.routerlogin.net
Model Name	R8500



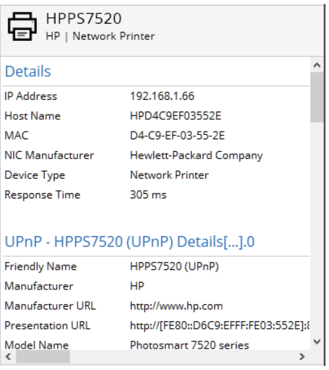
Dell Latitude E7450
Dell | Windows Device

Details

IP Address	192.168.1.115
Host Name	RMT-1290
MAC	10-02-B5-3A-C5-4B
NIC Manufacturer	Intel Corporation
Device Type	Windows Device
Response Time	0 ms

System Details:

Machine Name	Dell Latitude E7450
Machine Mfg	Dell
Machine Serial	CSY6H72



HPPS7520
HP | Network Printer

Details

IP Address	192.168.1.66
Host Name	HPD4C9EF03552E
MAC	D4-C9-EF-03-55-2E
NIC Manufacturer	Hewlett-Packard Company
Device Type	Network Printer
Response Time	305 ms

UPnP - HPPS7520 (UPnP) Details[...].0

Friendly Name	HPPS7520 (UPnP)
Manufacturer	HP
Manufacturer URL	http://www.hp.com
Presentation URL	http://[FE80::D6C9:EFFF:FE03:552E]:8
Model Name	Photosmart 7520 series

Gateway	Local Device (computer)	Network Device (network printer)

For discovered devices, the Network Devices scanner provides the following capabilities:

- Detailed technical information (e.g. IP address, MAC Address, Host Name, UPnP/WSD/WCN details, etc.) in the right-hand details pane
    - **Note:** A right-click context menu is available with the following functionality:
        - Copy to clipboard
        - Open in default web browser (for URL based content)
        - Search the internet for…
        - Edit Cell (for Device Name, Manufacturer, MAC Address and Device Type only)
- **Configure** a network device by jumping out to its web GUI (on supported devices only)
    - **Please note:** The device must advertise a SSDP/UPnP/WCN/WSD Presentation URL
- **Ping** a device
- **Export** results to the clipboard, text file, or CSV

Configuration

This section provides information about how your networking is configured as a whole. Access is provided to the *ping* and *tracert* networking utilities. Network shares are also available here for inspection. Please note that network shares may include shares which are available only to network admins and programs/utilities which have *SYSTEM* permissions.

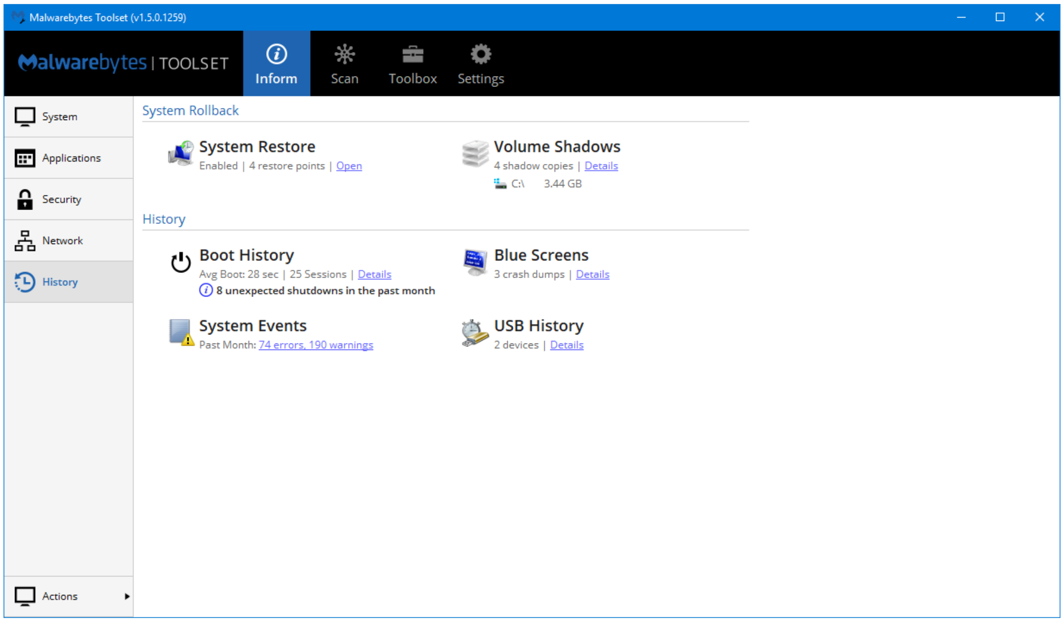
If the computer is configured to utilize a proxy server for access to the Internet, that can be inspected here using the Windows Internet Properties dialog. The Hosts file can be inspected here as well. This file is modifiable by the user, and is used by Windows to redirect Internet URL's to non-standard IP addresses, or to block access to troublesome URL's. This file is sometimes modified by malware as well.

Network Adapters

This section shows presence and configuration of network adapters, including adapters used in a virtual machine environment. You may inspect properties of each adapter. Of special interest here is the display of each adapter's IP address, and the method by which each adapter obtains its IP address. If there is a loss in connectivity on a machine using Dynamic Host Configuration Protocol (DHCP), the IP address will often show a 169.254.x.x IP address. This address range indicates an inability to receive an IP address from the network's DHCP server.

History tab

This tab provides tools used for disaster recovery, as well as the ability to inspect details on anomalies that the computer has encountered. A screenshot is shown below.



System Rollback

System Restore
Enabled | 4 restore points | Open

Volume Shadows
4 shadow copies | Details
C:\ 3.44 GB

History

Boot History
Avg Boot: 28 sec | 25 Sessions | Details
8 unexpected shutdowns in the past month

Blue Screens
3 crash dumps | Details

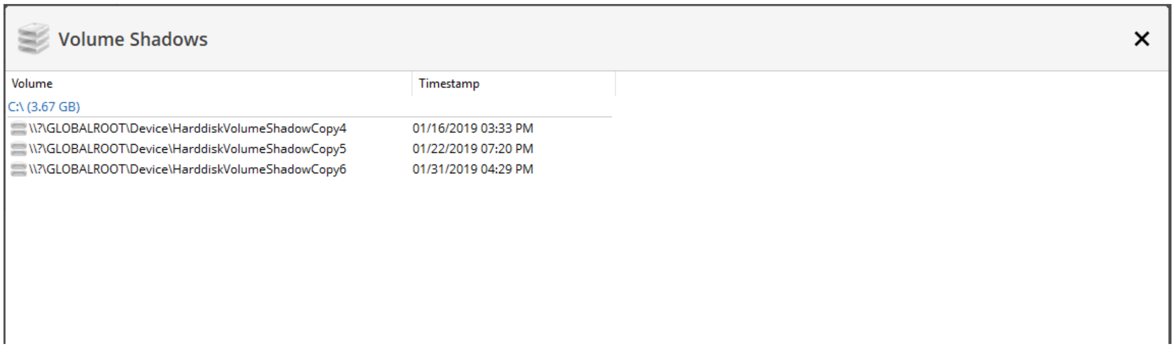
System Events
Past Month: 74 errors, 190 warnings

USB History
2 devices | Details

System Rollback

This section is focused specifically on disaster recovery measures which have been taken on the computer. **System Restore** points are commonly created prior to Windows updates, and may also be created prior to installation of any application which incorporates this process. If you encounter a serious error on your computer, restore points may provide the most effective answer.

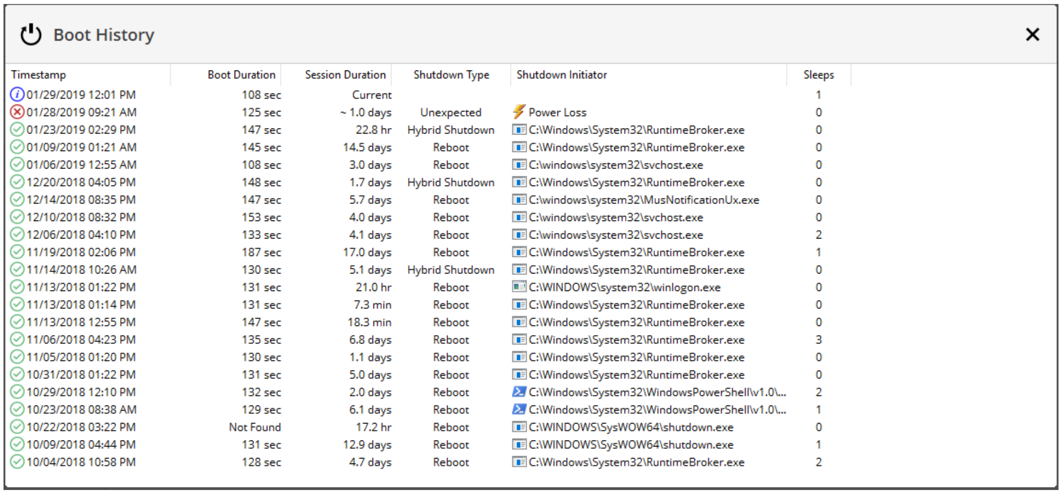
Volume Shadows are used to create snapshots of system files. If problems are encountered with a file which uses this service, it can be rolled back to a previous version. The rollback process uses the Previous Versions tab of a file's Properties page.



Volume	Timestamp
C:\ (3.67 GB)	
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy4	01/16/2019 03:33 PM
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy5	01/22/2019 07:20 PM
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy6	01/31/2019 04:29 PM

History

This section focuses on status of the computer with regard to its daily operations. Boot History has an entry for each time the computer has been started/restarted, which includes the length of time required to boot the computer to a fully operational state, as well as how long that session lasted. A copy of Boot History Details is shown below.



Boot History

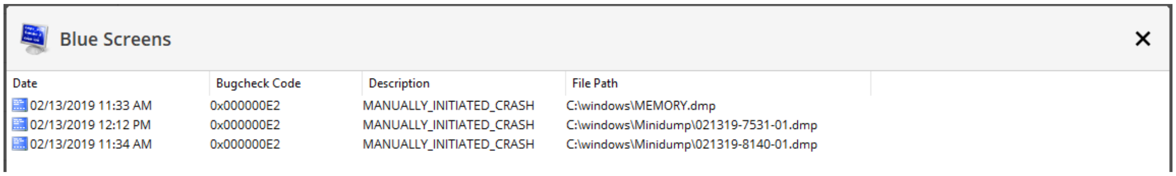
Timestamp	Boot Duration	Session Duration	Shutdown Type	Shutdown Initiator	Sleeps
ⓘ 01/29/2019 12:01 PM	108 sec	Current			1
✗ 01/28/2019 09:21 AM	125 sec	~ 1.0 days	Unexpected	Power Loss	0
✓ 01/23/2019 02:29 PM	147 sec	22.8 hr	Hybrid Shutdown	C:\Windows\System32\RuntimeBroker.exe	0
✓ 01/09/2019 01:21 AM	145 sec	14.5 days	Reboot	C:\Windows\System32\RuntimeBroker.exe	0
✓ 01/06/2019 12:55 AM	108 sec	3.0 days	Reboot	C:\windows\system32\svchost.exe	0
✓ 12/20/2018 04:05 PM	148 sec	1.7 days	Hybrid Shutdown	C:\Windows\System32\RuntimeBroker.exe	0
✓ 12/14/2018 08:35 PM	147 sec	5.7 days	Reboot	C:\windows\system32\MusNotificationUx.exe	0
✓ 12/10/2018 08:32 PM	153 sec	4.0 days	Reboot	C:\windows\system32\svchost.exe	0
✓ 12/06/2018 04:10 PM	133 sec	4.1 days	Reboot	C:\windows\system32\svchost.exe	2
✓ 11/19/2018 02:06 PM	187 sec	17.0 days	Reboot	C:\Windows\System32\RuntimeBroker.exe	1
✓ 11/14/2018 10:26 AM	130 sec	5.1 days	Hybrid Shutdown	C:\Windows\System32\RuntimeBroker.exe	0
✓ 11/13/2018 01:22 PM	131 sec	21.0 hr	Reboot	C:\WINDOWS\system32\winlogon.exe	0
✓ 11/13/2018 01:14 PM	131 sec	7.3 min	Reboot	C:\Windows\System32\RuntimeBroker.exe	0
✓ 11/13/2018 12:55 PM	147 sec	18.3 min	Reboot	C:\Windows\System32\RuntimeBroker.exe	0
✓ 11/06/2018 04:23 PM	135 sec	6.8 days	Reboot	C:\Windows\System32\RuntimeBroker.exe	3
✓ 11/05/2018 01:20 PM	130 sec	1.1 days	Reboot	C:\Windows\System32\RuntimeBroker.exe	0
✓ 10/31/2018 01:22 PM	131 sec	5.0 days	Reboot	C:\Windows\System32\RuntimeBroker.exe	0
✓ 10/29/2018 12:10 PM	132 sec	2.0 days	Reboot	C:\Windows\System32\WindowsPowerShell\v1.0\...	2
✓ 10/23/2018 08:38 AM	129 sec	6.1 days	Reboot	C:\Windows\System32\WindowsPowerShell\v1.0\...	1
✓ 10/22/2018 03:22 PM	Not Found	17.2 hr	Reboot	C:\WINDOWS\SysWOW64\shutdown.exe	0
✓ 10/09/2018 04:44 PM	131 sec	12.9 days	Reboot	C:\WINDOWS\SysWOW64\shutdown.exe	1
✓ 10/04/2018 10:58 PM	128 sec	4.7 days	Reboot	C:\Windows\System32\RuntimeBroker.exe	2

In this screenshot, each column was compressed so that more information could be displayed. Note the *Timestamp* column. Each entry is preceded by an icon. Those icons are explained below.

ⓘ	The session currently in progress.
✓	A past session which terminated by either a reboot or planned shutdown.
✗	A past session which terminated abnormally (e.g. power failure, forced shutdown, system crash)

When System Events statistics are clicked, Windows Event Viewer opens with a special filter to view only Errors and Warnings. This allows you to view information pertaining to every critical system event which has occurred in the life of the system. Operating systems prior to Vista had a maximum file size limitation (300 megabytes), though this likely caused no issues for users of this information.

Blue Screens tells you how many memory dumps (mini and full) were performed as a result of system crashes (aka BSODs). Click **Details** to launch a window with details on the detected crash dump including the Date, Bugcheck Code, Description, and File Path to the crash dump file.



Blue Screens

Date	Bugcheck Code	Description	File Path
02/13/2019 11:33 AM	0x000000E2	MANUALLY_INITIATED_CRASH	C:\windows\MEMORY.dmp
02/13/2019 12:12 PM	0x000000E2	MANUALLY_INITIATED_CRASH	C:\windows\Minidump\021319-7531-01.dmp
02/13/2019 11:34 AM	0x000000E2	MANUALLY_INITIATED_CRASH	C:\windows\Minidump\021319-8140-01.dmp

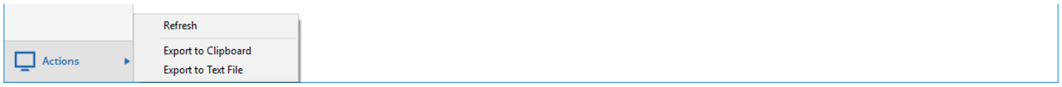
Please note that not all crashes have the ability to create a dump file. There is no facility provided here to evaluate the dump files. External Windows utilities must be used for that purpose.

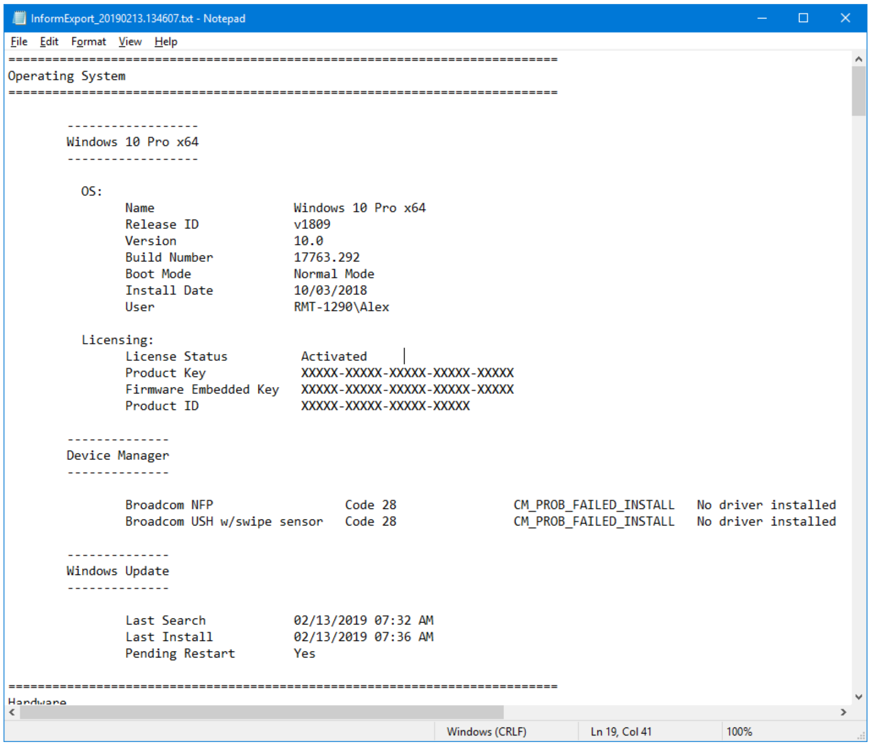
The **USB History** section shows the most recent insertion of each USB drive that has been used in the computer. Please note that entries may appear to be redundant when multiple USB drives made by the same manufacturer have been inserted. This is because of the method that different vendors use to report the drive's insertion to the operating system. Windows will assign each USB drive its own GUID, providing a unique identity. Please note that information shown is specifically with regard to drive insertion, and not to drive contents and how they were used.

Actions

This button opens a menu with options to control certain actions with Inform. Here is an overview of the available actions:

- Refresh – Force a re-scan of the device and update all applicable areas of Inform.
- Export to Clipboard – Export current results of Inform in plain text to the clipboard.
- Export to Text File – Export current results of Inform in plain text to a file of your choosing.

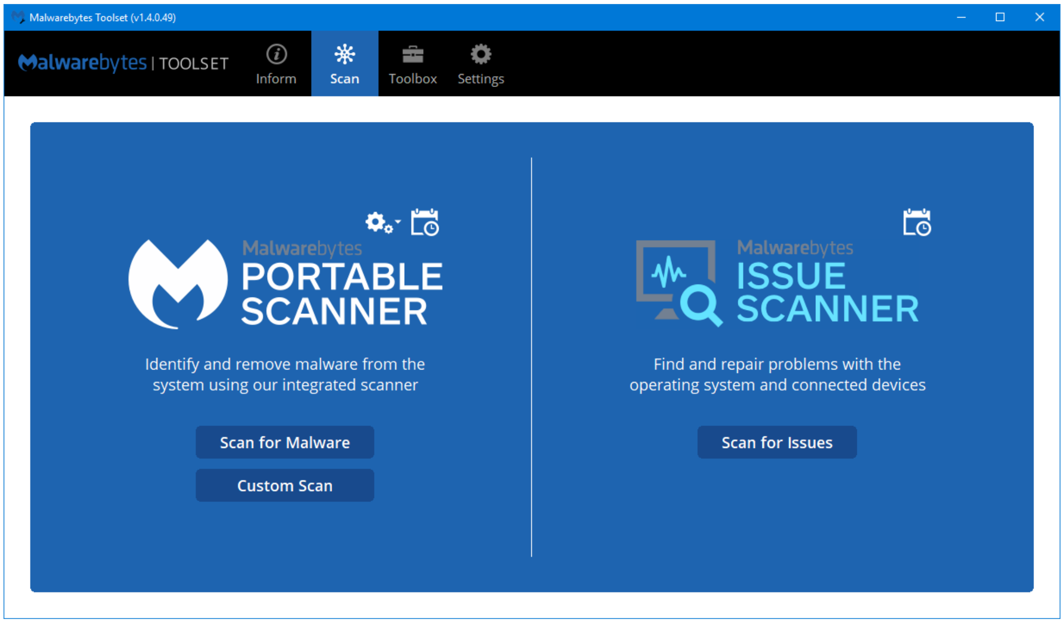



InformExport_20190213.134607.txt - Notepad
File Edit Format View Help
Windows (CRLF)
Ln 19, Col 41
100%

```
===========================================================================
Operating System
===========================================================================


        ------------------
        Windows 10 Pro x64
        ------------------

          OS:
                Name                   Windows 10 Pro x64
                Release ID             v1809
                Version                10.0
                Build Number           17763.292
                Boot Mode              Normal Mode
                Install Date           10/03/2018
                User                   RMT-1290\Alex

          Licensing:
                License Status          Activated
                Product Key             XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
                Firmware Embedded Key   XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
                Product ID              XXXXX-XXXXX-XXXXX-XXXXX

        --------------
        Device Manager
        --------------

                Broadcom NFP                  Code 28                 CM_PROB_FAILED_INSTALL   No driver installed
                Broadcom USH w/swipe sensor   Code 28                 CM_PROB_FAILED_INSTALL   No driver installed

        --------------
        Windows Update
        --------------

                Last Search            02/13/2019 07:32 AM
                Last Install           02/13/2019 07:36 AM
                Pending Restart        Yes

===========================================================================
Hardware
```

Scan

This program module contains two types of wizard-based diagnostic scanners – the *Malwarebytes Portable Scanner* to remove malware, PUPs and PUMs, and the *Malwarebytes Issue Scanner* to fix Windows OS and device related issues.


Malwarebytes Toolset (v1.4.0.49)
Malwarebytes | TOOLSET
Inform
Scan
Toolbox
Settings
Malwarebytes
PORTABLE SCANNER
Identify and remove malware from the system using our integrated scanner
Scan for Malware
Custom Scan
Malwarebytes
ISSUE SCANNER
Find and repair problems with the operating system and connected devices
Scan for Issues

The *Malwarebytes Portable Scanner* requires Windows 7 and higher as well as .NET 4.5. If it is not installed (or has been rendered unusable due to malware), please use the *Malwarebytes Breach Remediation* command-line utility included in the Toolset at:

```
Malwarebytes\MBBRv2\MBBR.exe
```

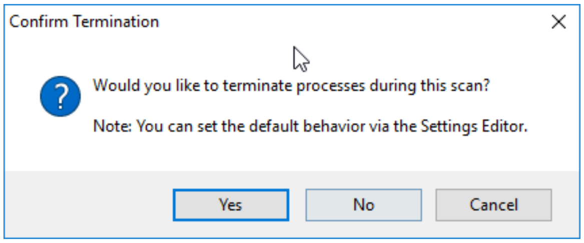
Malwarebytes Portable Scanner

This option scans the computer for malware, based on selection criteria provided by the user. The *Malwarebytes Portable Scanner* uses the *Malwarebytes for Windows version 3.6.1* engine, offering full scanning and remediation functionality of our flagship product without the need to install *Malwarebytes* itself.

Malware, PUPs and PUMs often fills the screen with windows, which tends to get in the way of troubleshooting efforts. For this reason, *Malwarebytes Toolset* provides the option of killing running processes while a scan is running. Known-good processes, processes not typically targeted by malware, and processes used by *Malwarebytes Toolset* are exempt from forced termination. You may add your own tools to this whitelist as well. More on that later.

Scan for Malware

When the Scan for Malware button is pressed, the screen shown below is presented over the top of the existing screen.



Confirm Termination

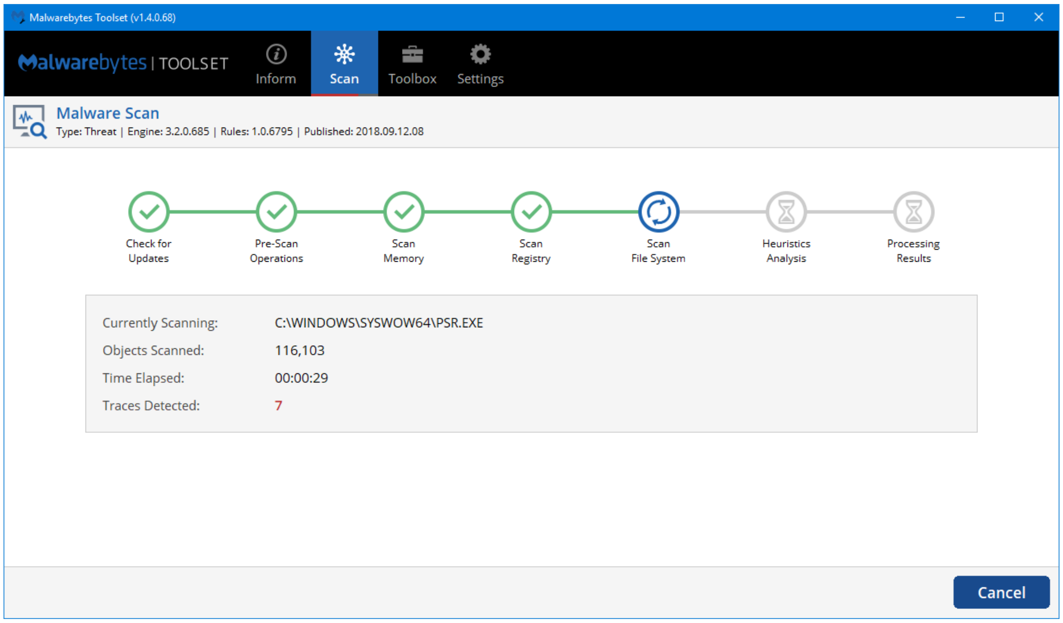
Would you like to terminate processes during this scan?

Note: You can set the default behavior via the Settings Editor.

You may choose **Cancel** to return to the previous screen. Click **Yes** to terminate running processes, or click **No** to allow running processes to continue running.

Here, you may choose to terminate running processes during the scan or allow them to continue operation. After either of these buttons are pressed, the scan will begin.

Malwarebytes Toolset uses a <u>Threat</u> scan as a default scan. This scan method analyzes all areas of the computer which are typically associated with malware outbreaks. A screenshot of a scan in progress is shown below.



Malware Scan

Type: Threat | Engine: 3.2.0.685 | Rules: 1.0.6795 | Published: 2018.09.12.08

Currently Scanning: C:\WINDOWS\SYSWOW64\PSR.EXE
Objects Scanned: 116,103
Time Elapsed: 00:00:29
Traces Detected: 7

After a scan is requested and before it actually starts, *Malwarebytes Toolset* connects to Malwarebytes infrastructure servers to request and receive the latest protection updates. If the computer has no Internet connectivity or active malware prevents this step, the Toolset will attempt to use protection updates that were downloaded during a previous scan. If existing updates are not available, you must perform an update using another computer.

► **On first use of the Malwarebytes Toolset, downloading protection updates are mandatory**.

While a scan is running, *Malwarebytes Toolset* displays several icons on the main screen which serve as progress indicators for the scan. These are as follows:

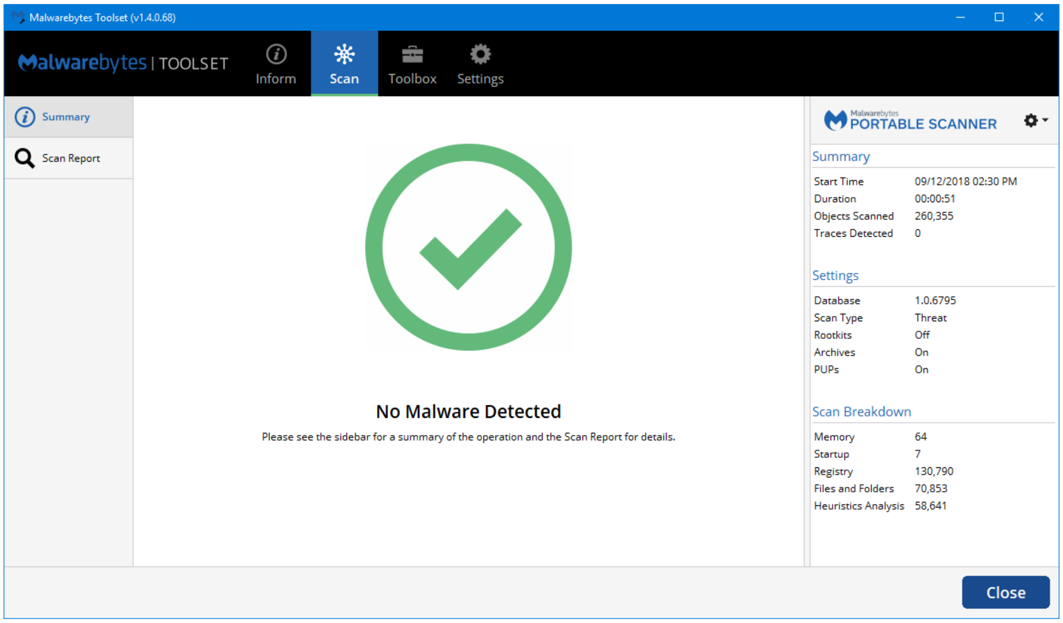
- **Grey hourglass –** Scan phase not yet executed; will be replaced by either a blue circular animation or a green hyphen
- **Green hyphen –** Scan phase not performed (hyper scan and custom scan do not execute all phases)
- **Blue circular animation –** Scan phase currently running; will be replaced by a green checkmark when complete
- **Green checkmark –** Scan phase completed

A light blue bar immediately under the Scan button in the menu pane will also show scan progress. It is difficult to notice, so it has been supplemented by indicators in the Windows taskbar, as shown below.

When a scan is running, a green indicator shows scan progress.

Because malware was detected during the scan, the icon is replaced by red as its final status. When malware is detected during execution of the scan, this icon will immediately switch from green to red.

When a scan completes without malware being detected, you will see the Summary as shown here.



No Malware Detected

Please see the sidebar for a summary of the operation and the Scan Report for details.

Summary

Start Time	09/12/2018 02:30 PM
Duration	00:00:51
Objects Scanned	260,355
Traces Detected	0

Settings

Database	1.0.6795
Scan Type	Threat
Rootkits	Off
Archives	On
PUPs	On

Scan Breakdown

Memory	64
Startup	7
Registry	130,790
Files and Folders	70,853
Heuristics Analysis	58,641

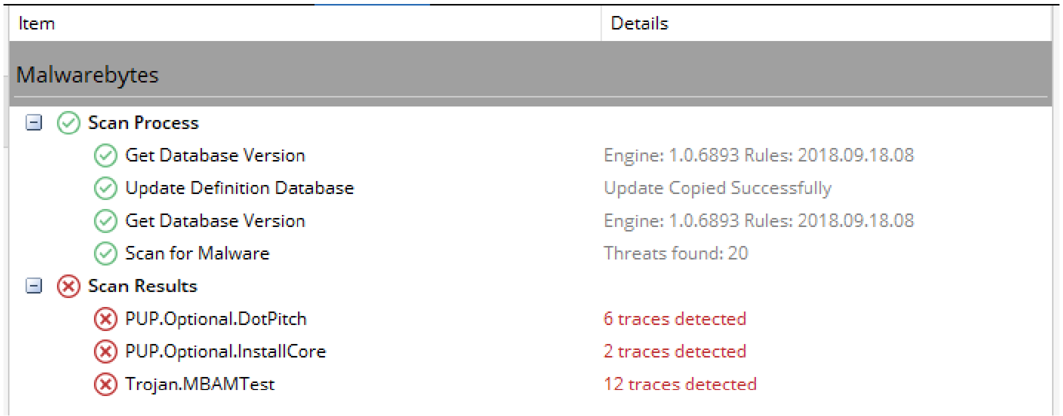
Status Icons

Several large icons are used to inform you of scan status, here and in the Issue Scanner (which will be discussed later). These icons are oversized, so that you can easily see status without forcing you to interrupt your repair work. These are the icons used and their meaning.

✓	No issues were detected
!	Non-critical issues which require your attention were detected during the scan
✗	Critical issues which require your attention were detected during the scan
⏻	A reboot is required to complete the repair process

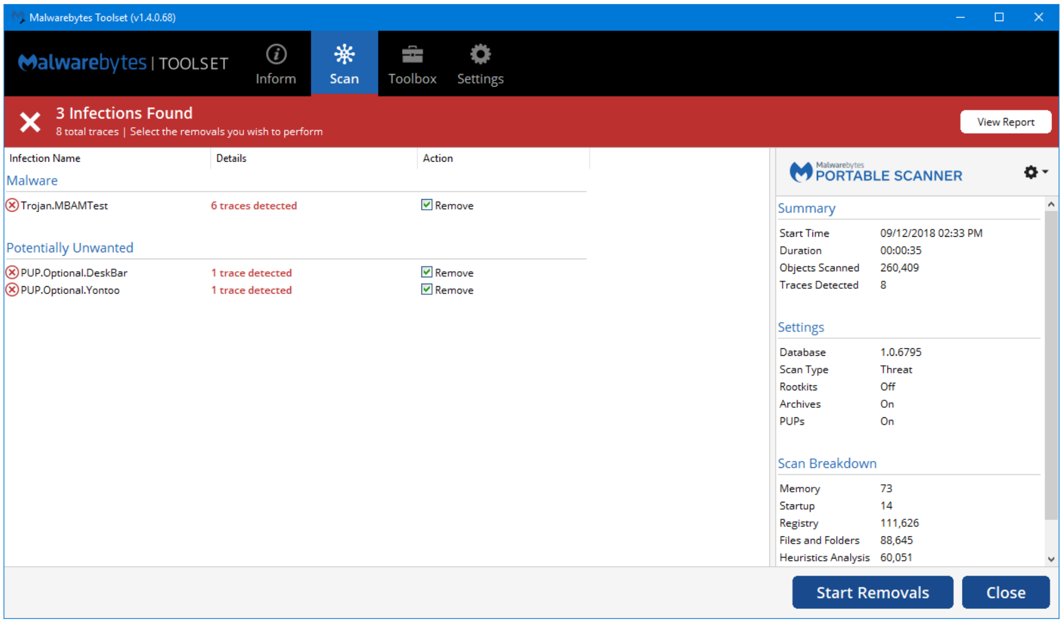
Icons will always be in a color which represents the most serious situation. If all but one of the items tested passed, the icon shown will be in the color which represents either a critical or non-critical issue.

You may also inspect the Scan Report to look at other information pertaining to the scan.



Item	Details
Malwarebytes	
⊟ Scan Process	
Get Database Version	Engine: 1.0.6893 Rules: 2018.09.18.08
Update Definition Database	Update Copied Successfully
Get Database Version	Engine: 1.0.6893 Rules: 2018.09.18.08
Scan for Malware	Threats found: 20
⊟ Scan Results	
PUP.Optional.DotPitch	6 traces detected
PUP.Optional.InstallCore	2 traces detected
Trojan.MBAMTest	12 traces detected

The following screenshot shows results after a custom scan which detected malware.


Malwarebytes Toolset (v1.4.0.68)
Malwarebytes | TOOLSET
Inform
Scan
Toolbox
Settings

3 Infections Found

8 total traces | Select the removals you wish to perform

Infection Name	Details	Action
Malware		
Trojan.MBAMTest	6 traces detected	☑ Remove
Potentially Unwanted		
PUP.Optional.DeskBar	1 trace detected	☑ Remove
PUP.Optional.Yontoo	1 trace detected	☑ Remove

Malwarebytes PORTABLE SCANNER

Summary

Start Time	09/12/2018 02:33 PM
Duration	00:00:35
Objects Scanned	260,409
Traces Detected	8

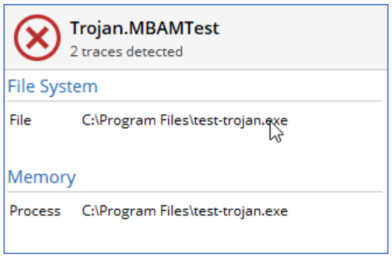
Settings

Database	1.0.6795
Scan Type	Threat
Rootkits	Off
Archives	On
PUPs	On

Scan Breakdown

Memory	73
Startup	14
Registry	111,626
Files and Folders	88,645
Heuristics Analysis	60,051

The left section of the screen shows malware and PUPs/PUMs which were detected, the number of traces detected, and checkboxes to allow you to select which malware to remove.



Trojan.MBAMTest

2 traces detected

File System

File	C:\Program Files\test-trojan.exe

Memory

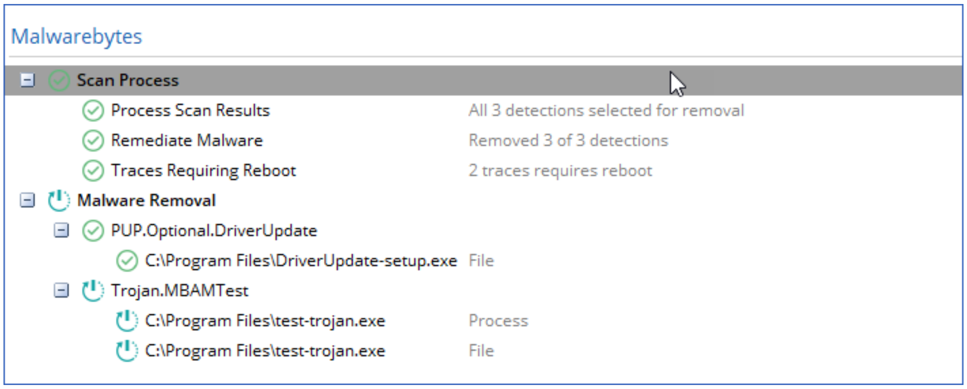
Process	C:\Program Files\test-trojan.exe

Selecting this malware causes the Summary (right) section of the screen to display the information shown here.

Traces is a new term. It is the number of specific vectors which a threat is using to attack your computer. The *Trojan.MBAMTest* malware has two traces, the directory where the file is stored, and memory which the running program occupied. If processes were terminated during

View Report provides a display which is best described as a hybrid between a “clean” Scan Report screen combined with a “dirty” Scan Summary screen. If needed, you can click the gear icon in the top of the Summary section and select to copy the results to the clipboard or export a text file.

Once you have reviewed scan results, you may click **Start Removals** to initiate the threat removal process. After performing the removal process, a Repair Report will be displayed in its expanded form. If needed, you can copy information listed in the Scan Results, Scan Summary, Scan Report or Repair Report by right-clicking an item and selecting the content to copy. You can also use the gear icon in the Summary section to export the a detailed summary to the clipboard or a text file.

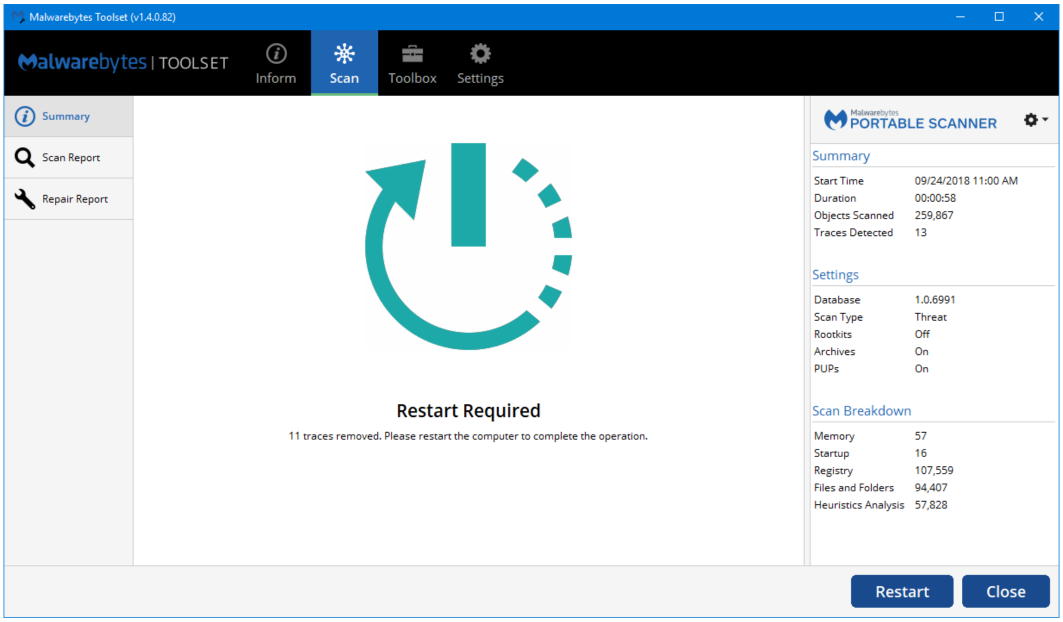


Malwarebytes

Scan Process	
Process Scan Results	All 3 detections selected for removal
Remediate Malware	Removed 3 of 3 detections
Traces Requiring Reboot	2 traces requires reboot
Malware Removal	
PUP.Optional.DriverUpdate	
C:\Program Files\DriverUpdate-setup.exe	File
Trojan.MBAMTest	
C:\Program Files\test-trojan.exe	Process
C:\Program Files\test-trojan.exe	File

Delete on Reboot

If a reboot is required to remove any threat, you will be presented the applicable status icon with a Restart button to initiate the reboot process and a Close button if you need to manually reboot the PC later.



Restart Required

11 traces removed. Please restart the computer to complete the operation.

Summary

Start Time	09/24/2018 11:00 AM
Duration	00:00:58
Objects Scanned	259,867
Traces Detected	13

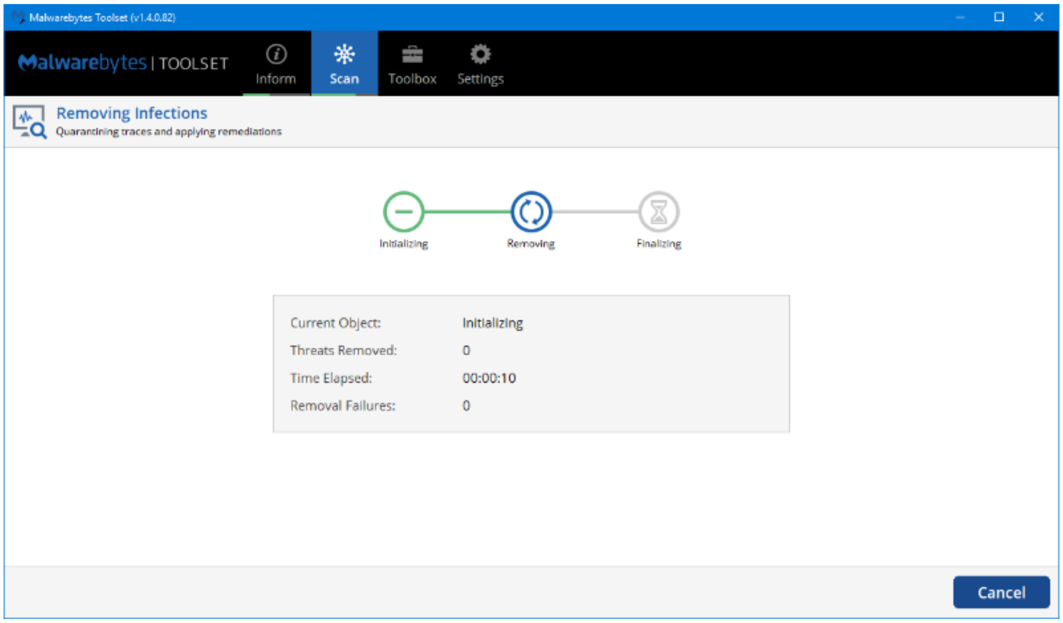
Settings

Database	1.0.6991
Scan Type	Threat
Rootkits	Off
Archives	On
PUPs	On

Scan Breakdown

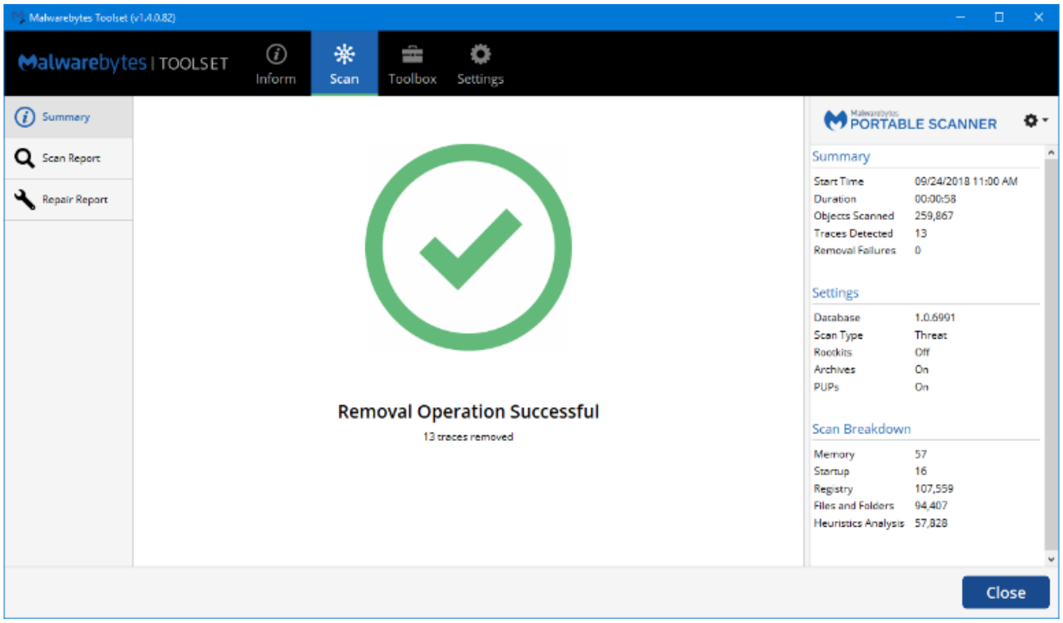
Memory	57
Startup	16
Registry	107,559
Files and Folders	94,407
Heuristics Analysis	57,828

In any event, the Toolset will automatically relaunch after reboot and once a user account logs in. This will start the post-reboot removal progress window before going to a final Summary of the entire operation.



Removing Infections
Quarantining traces and applying remediations

Current Object:	Initializing
Threats Removed:	0
Time Elapsed:	00:00:10
Removal Failures:	0



Removal Operation Successful
13 traces removed

Summary

Start Time	09/24/2018 11:00 AM
Duration	00:00:58
Objects Scanned	259,867
Traces Detected	13
Removal Failures	0

Settings

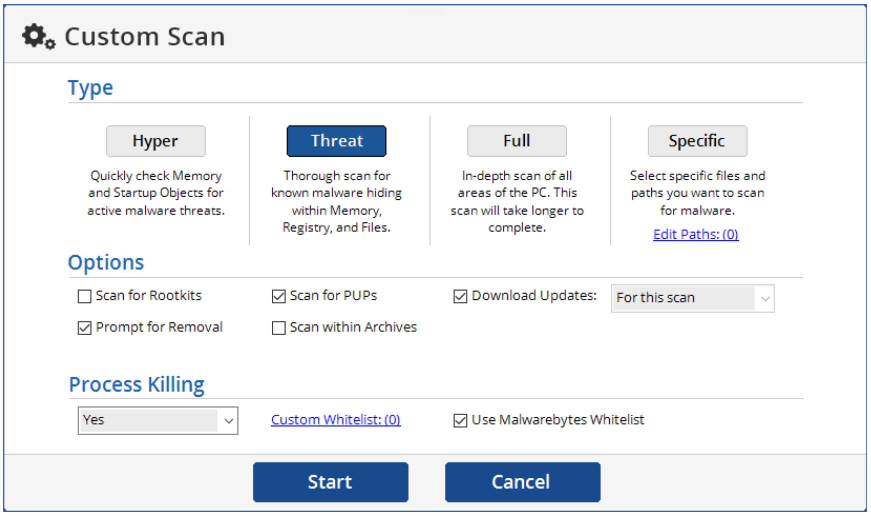
Database	1.0.6991
Scan Type	Threat
Rootkits	Off
Archives	On
PUPs	On

Scan Breakdown

Memory	57
Startup	16
Registry	107,559
Files and Folders	94,407
Heuristics Analysis	57,828

Custom Scan

The second scan mode available in *Malwarebytes Toolset* is the custom scan. Click **Custom Scan** to launch this screen over the top of the *Malwarebytes Toolset* screen.



Custom Scan

Type

Hyper: Quickly check Memory and Startup Objects for active malware threats.

Threat: Thorough scan for known malware hiding within Memory, Registry, and Files.

Full: In-depth scan of all areas of the PC. This scan will take longer to complete.

Specific: Select specific files and paths you want to scan for malware. Edit Paths: (0)

Options

☐ Scan for Rootkits
☑ Scan for PUPs
☑ Download Updates: For this scan
☑ Prompt for Removal
☐ Scan within Archives

Process Killing

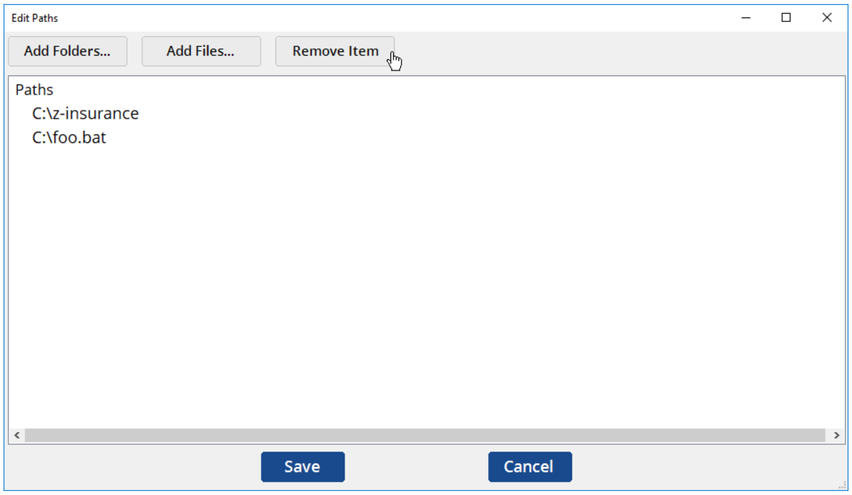
Yes
Custom Whitelist: (0)
☑ Use Malwarebytes Whitelist

Here you can pick the type of scan you wish to run, and the options you wish the scan to use. These settings are, for the most part, identical to the settings used in *Malwarebytes for Windows* and *Malwarebytes Breach Remediation CLI*. Under Process Killing, you may choose whether running processes should be killed. *Malwarebytes Toolset* uses a whitelist of known good processes to be excluded from potential termination, and you may add your own through use of a *Custom Whitelist*.

If you choose not to use the *Malwarebytes Whitelist* here, you will not cause your computer to crash. Windows system processes will continue to function as intended. Non-critical applications (such as browsers or email programs) would be terminated if a whitelist is not used.

When running a Specific scan, click **Edit Paths** to select specific files or folders which should be scanned. In the screenshot below, **Add Folders…** was used to add a specific folder to scan, and **Add Files…** was used to select a single file. To remove a file or folder from the list, highlight the item to remove and click **Remove Item**.

Malware may exist in files and in processes running in memory. When running a scan on a computer for the first time, it is probably best to not kill processes, so that you have a clearer picture of the level of infection in that computer.

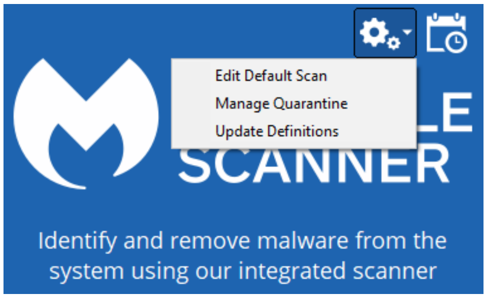


Edit Paths

Paths
C:\z-insurance
C:\foo.bat

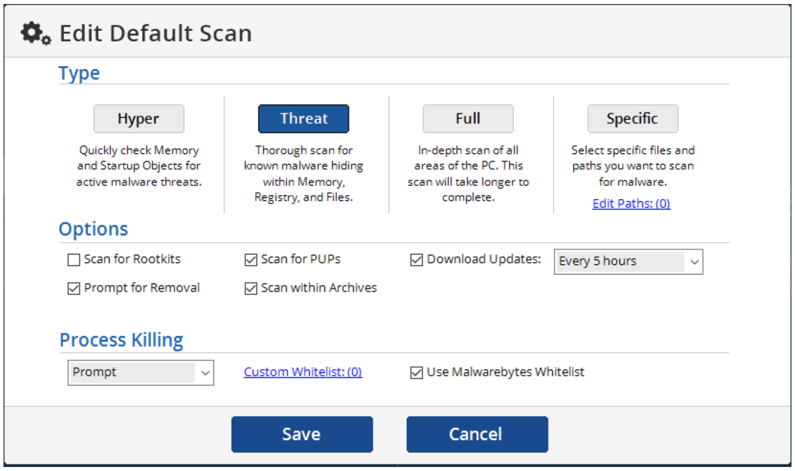
Settings, Quarantine, and Updates (Malwarebytes Portable Scanner)

You may have noticed the two gears above and to the right of the *Malwarebytes Portable Scanner* logo. This hides settings associated with the malware scanning component.



Identify and remove malware from the system using our integrated scanner

Edit Default Scan allows you to customize the default scanning experience for when you click **Scan for Malware**. When that option is selected, a screen identical to the Custom Scan screen (shown in the previous subsection) is displayed. Here, you can customize specifications of your default scan. This does not prevent you from running a Custom Scan with different specifications whenever you choose.



Edit Default Scan

Type

- Hyper: Quickly check Memory and Startup Objects for active malware threats.
- Threat: Thorough scan for known malware hiding within Memory, Registry, and Files.
- Full: In-depth scan of all areas of the PC. This scan will take longer to complete.
- Specific: Select specific files and paths you want to scan for malware. Edit Paths: (0)

Options

☐ Scan for Rootkits ☑ Scan for PUPs ☑ Download Updates: Every 5 hours

☑ Prompt for Removal ☑ Scan within Archives

Process Killing

Prompt Custom Whitelist: (0) ☑ Use Malwarebytes Whitelist

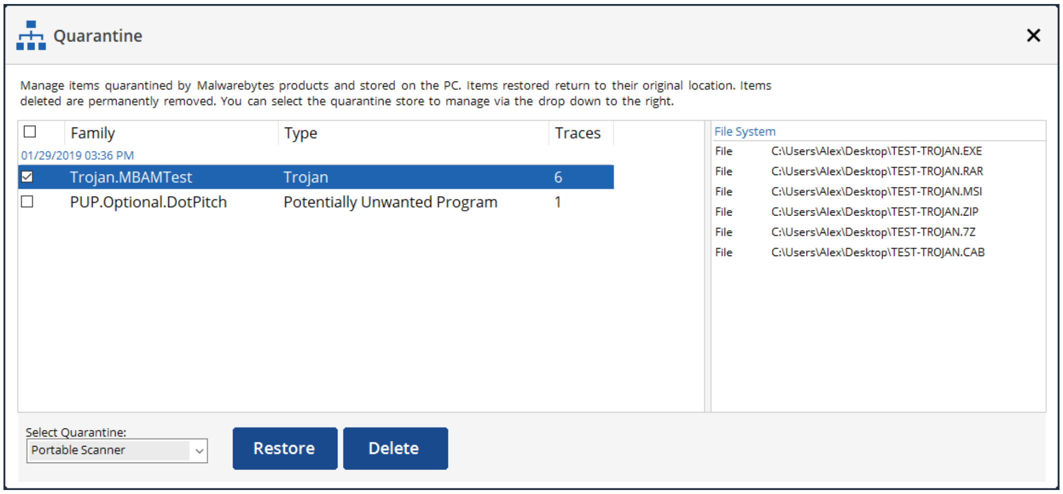
Manage Quarantine launches the Quarantine Manager, so you can delete or restore items that have been placed in the quarantine by the Malwarebytes Portable Scanner and the installed instance of the following Malwarebytes products:

- *Malwarebytes for Windows* (v 3.6.1+)
- *Malwarebytes Endpoint Protection*
- *Malwarebytes Breach Remediation* (v 3.6.1+)

Select Quarantine allows you to select the quarantine to interact with from a drop-down menu. By default, the Malwarebytes Portable Scanner quarantine is loaded when the Quarantine Manager is launched. The Quarantine Manager groups items by date of the scan and the family the traces belong to. This allows you to easily manage items by family, as they may be comprised of many traces, and mirror the reporting layout used by the Malwarebytes Portable Scanner.

The basic view will list the Family name, the Type of item, and the total number of Traces that comprise that item. To see the specific traces, simply click on it. That will populate a details side pane that lists all trace details. This includes type of trace and where it was found on the device.

If you want to manage an item, simply select the checkbox next to it then click the desired action. **Delete** will permanently delete all traces of that item and **Restore** will put all traces of that item back to their original location. You can select multiple items at once or select the top most checkbox to select all items in quarantine.



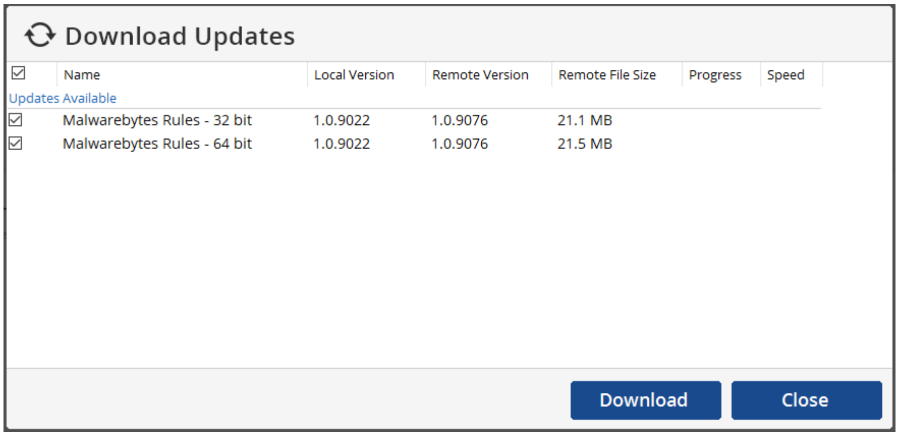
Manage items quarantined by Malwarebytes products and stored on the PC. Items restored return to their original location. Items deleted are permanently removed. You can select the quarantine store to manage via the drop down to the right.

□	Family	Type	Traces
01/29/2019 03:36 PM			
☑	Trojan.MBAMTest	Trojan	6
□	PUP.Optional.DotPitch	Potentially Unwanted Program	1

File System	
File	C:\Users\Alex\Desktop\TEST-TROJAN.EXE
File	C:\Users\Alex\Desktop\TEST-TROJAN.RAR
File	C:\Users\Alex\Desktop\TEST-TROJAN.MSI
File	C:\Users\Alex\Desktop\TEST-TROJAN.ZIP
File	C:\Users\Alex\Desktop\TEST-TROJAN.7Z
File	C:\Users\Alex\Desktop\TEST-TROJAN.CAB

Select Quarantine: Portable Scanner

Update Definitions allows manual update of the definition databases for the Malwarebytes Portable Scanner (64-bit and 32-bit). This option will launch a Download Updates (aka the MBTS Updater) window to check only for database updates. If updates are available, click **Download** and the MBTS Updater will acquire and install them for you.

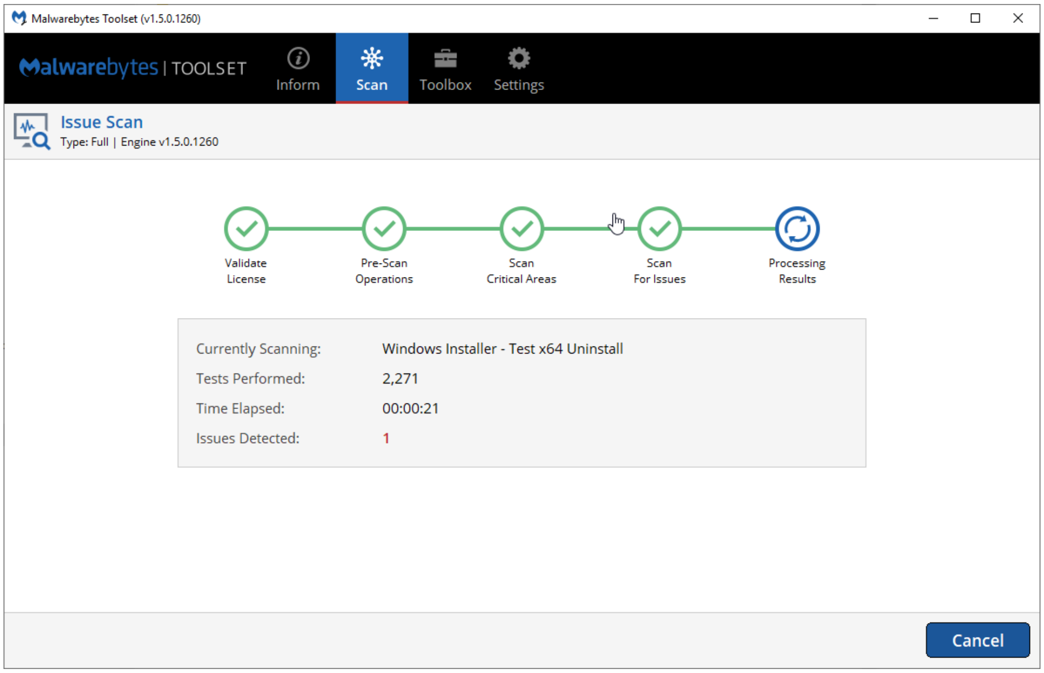


☑	Name	Local Version	Remote Version	Remote File Size	Progress	Speed
Updates Available						
☑	Malwarebytes Rules - 32 bit	1.0.9022	1.0.9076	21.1 MB		
☑	Malwarebytes Rules - 64 bit	1.0.9022	1.0.9076	21.5 MB		

Issue Scanner

Malwarebytes Toolset will initiate a scan of several system settings to help identify potential OS problems and hardware issues, then offer technical information on the issue or even offer an automated repair. These encompass disk drive errors, SMART Attributes, network connectivity problems, critical errors stored in Event Viewer, registry settings, files executed at startup, system services, Device Manager error codes and many other Windows settings. You can see a full list of the current Issue Scanners in the Malwarebytes Issue Scanner Technical Reference (https://malwarebytes.box.com/v/IssueScannerPDF). Below is a screenshot from Issue Scanner while it is scanning your system. The purpose of all icons used here are identical to the Portable Scanner.

- ▶ **This module is primarily designed for Vista and newer operating systems. It will detect a limited number of issues on Windows XP.**

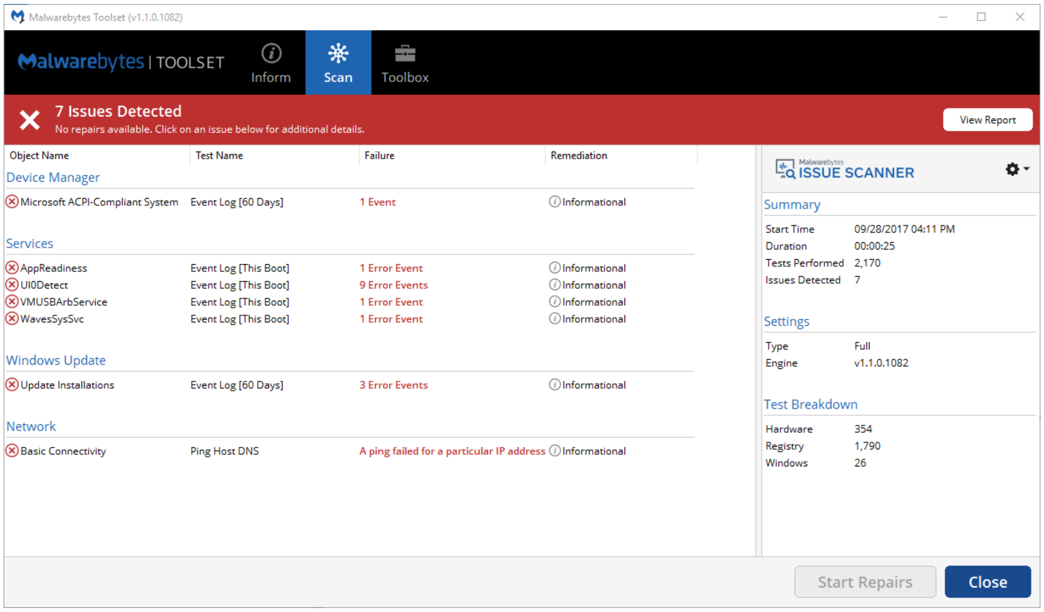


Issue Scan

Type: Full | Engine v1.5.0.1260

Currently Scanning:	Windows Installer - Test x64 Uninstall
Tests Performed:	2,271
Time Elapsed:	00:00:21
Issues Detected:	1

And here is a screenshot showing results of that scan.



7 Issues Detected

No repairs available. Click on an issue below for additional details.

Object Name	Test Name	Failure	Remediation
Device Manager			
⊗ Microsoft ACPI-Compliant System	Event Log [60 Days]	1 Event	ⓘ Informational
Services			
⊗ AppReadiness	Event Log [This Boot]	1 Error Event	ⓘ Informational
⊗ UI0Detect	Event Log [This Boot]	9 Error Events	ⓘ Informational
⊗ VMUSBArbService	Event Log [This Boot]	1 Error Event	ⓘ Informational
⊗ WavesSysSvc	Event Log [This Boot]	1 Error Event	ⓘ Informational
Windows Update			
⊗ Update Installations	Event Log [60 Days]	3 Error Events	ⓘ Informational
Network			
⊗ Basic Connectivity	Ping Host DNS	A ping failed for a particular IP address	ⓘ Informational

Summary

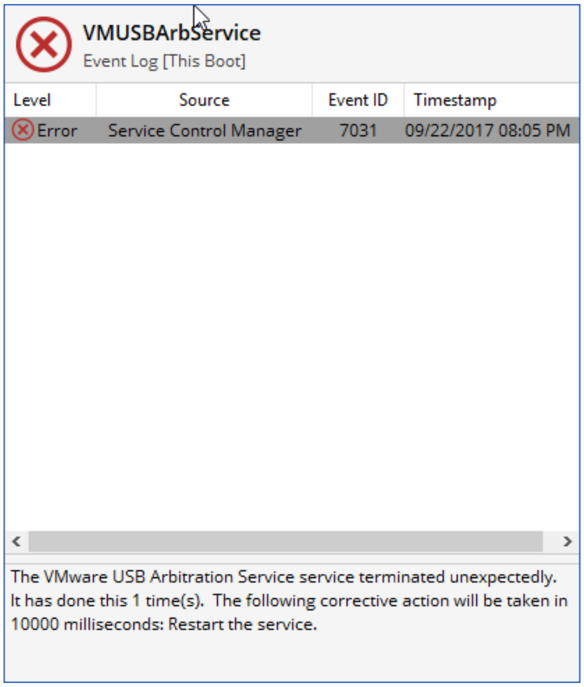
Start Time	09/28/2017 04:11 PM
Duration	00:00:25
Tests Performed	2,170
Issues Detected	7

Settings

Type	Full
Engine	v1.1.0.1082

Test Breakdown

Hardware	354
Registry	1,790
Windows	26



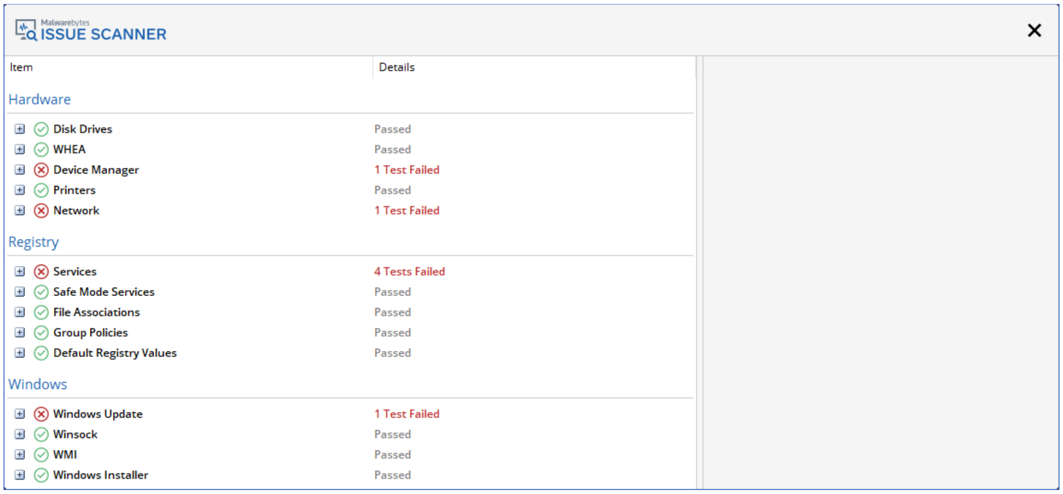
VMUSBArbService
Event Log [This Boot]

Level	Source	Event ID	Timestamp
⊗ Error	Service Control Manager	7031	09/22/2017 08:05 PM

The VMware USB Arbitration Service service terminated unexpectedly. It has done this 1 time(s). The following corrective action will be taken in 10000 milliseconds: Restart the service.

Highlighting any issue results in a more detailed explanation in the rightmost Details pane. The event description that you would typically read in the Windows Event Viewer is shown at the bottom of this pane.

You will notice that three issues were detected during this scan. Click **View Report** to see the results of all tests run during the Issue Scan. A high-level view is shown below. You can expand each of the items shown here to see exactly what the scan included. The full list of tests is too large to be included here. If needed, you can copy information listed in the Scan Results, Scan Summary, Scan Report or Repair Report by right clicking and item and selecting the content to copy.

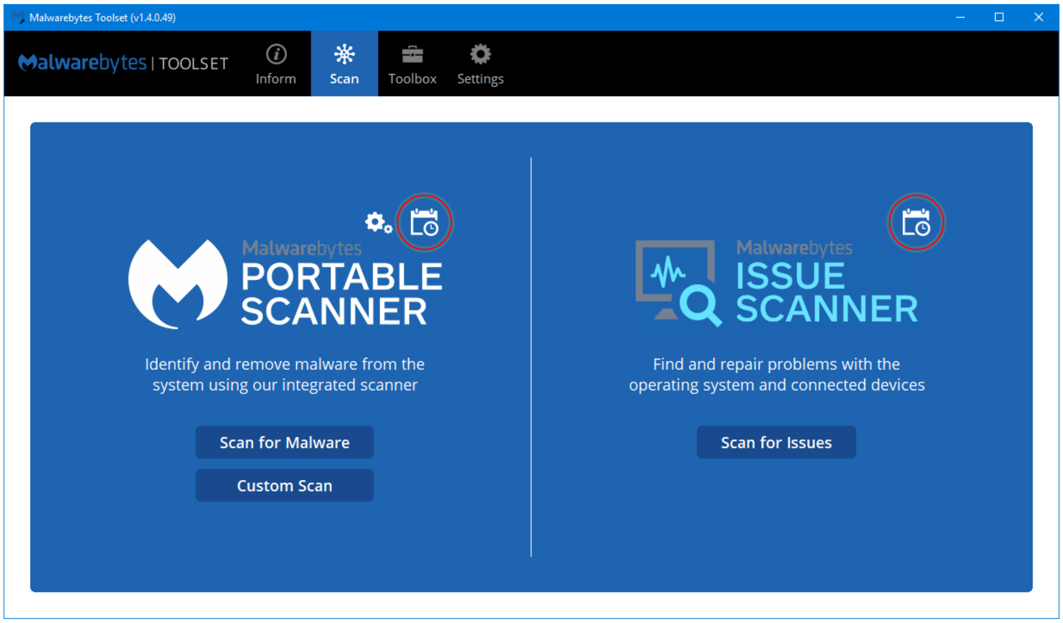


Item	Details
Hardware	
✓ Disk Drives	Passed
✓ WHEA	Passed
⊗ Device Manager	1 Test Failed
✓ Printers	Passed
⊗ Network	1 Test Failed
Registry	
⊗ Services	4 Tests Failed
✓ Safe Mode Services	Passed
✓ File Associations	Passed
✓ Group Policies	Passed
✓ Default Registry Values	Passed
Windows	
⊗ Windows Update	1 Test Failed
✓ Winsock	Passed
✓ WMI	Passed
✓ Windows Installer	Passed

Finally, it is important to note that these may not be problems. *Malwarebytes Toolset* has analyzed typical settings on many Windows environments (both operating system and service pack permutations) to determine what is expected. A knowledgeable user may modify settings on their computer, and a computer used in a business environment may have been fine-tuned by their IT group. When issues *are* detected, further investigation is warranted.

Scan History

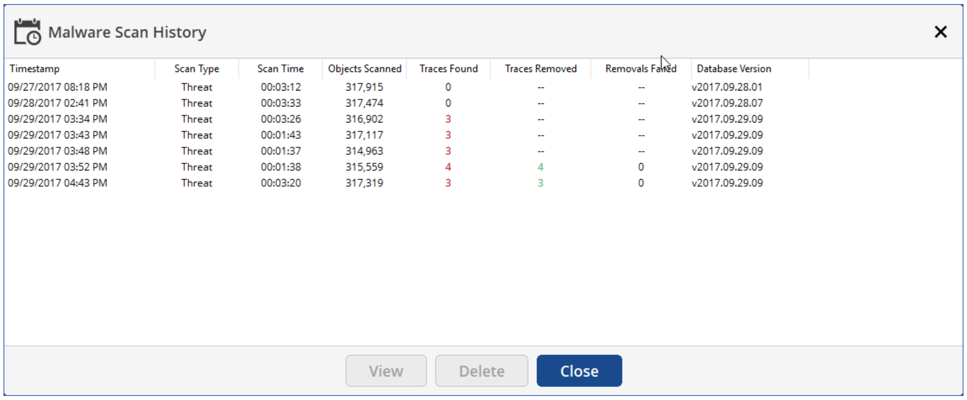
Malware scans and issue scans both generate history logs, allowing inspection of the results of each scan that has been executed. Please note the location of the calendar icons on the Scan screen shown below.



Identify and remove malware from the system using our integrated scanner

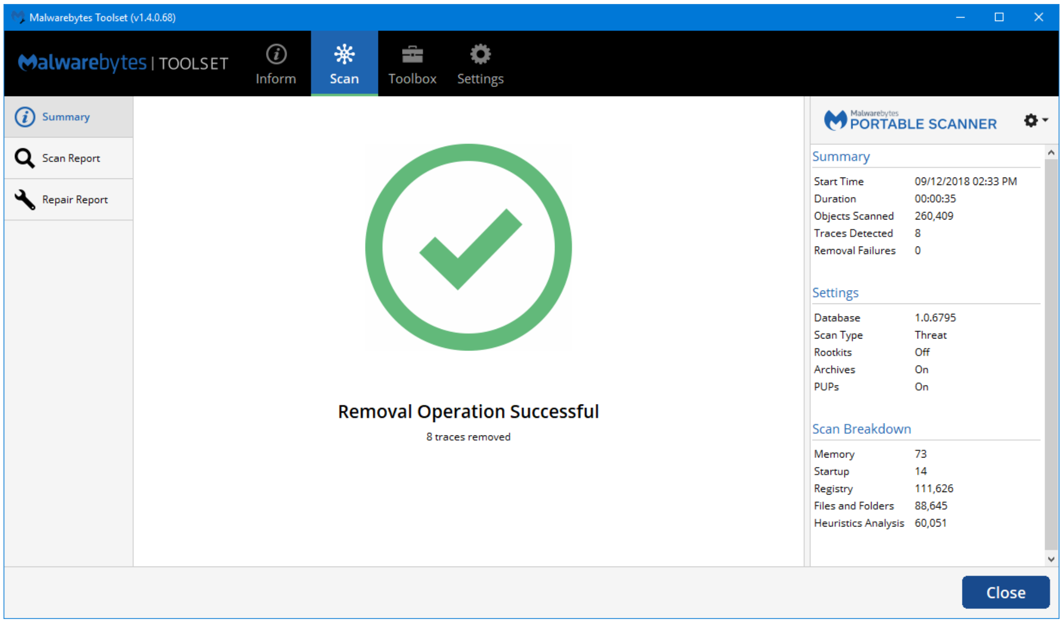
Find and repair problems with the operating system and connected devices

Clicking either calendar icon displays a history of the scans of the type selected which have been executed. A Malware Scan History Log is shown below.



Timestamp	Scan Type	Scan Time	Objects Scanned	Traces Found	Traces Removed	Removals Failed	Database Version
09/27/2017 08:18 PM	Threat	00:03:12	317,915	0	--	--	v2017.09.28.01
09/28/2017 02:41 PM	Threat	00:03:33	317,474	0	--	--	v2017.09.28.07
09/29/2017 03:34 PM	Threat	00:03:26	316,902	3	--	--	v2017.09.29.09
09/29/2017 03:43 PM	Threat	00:01:43	317,117	3	--	--	v2017.09.29.09
09/29/2017 03:48 PM	Threat	00:01:37	314,963	3	--	--	v2017.09.29.09
09/29/2017 03:52 PM	Threat	00:01:38	315,559	4	4	0	v2017.09.29.09
09/29/2017 04:43 PM	Threat	00:03:20	317,319	3	3	0	v2017.09.29.09

Selecting the first entry on this page causes the results of this scan to be displayed, as shown below.



Removal Operation Successful

8 traces removed

Summary

Start Time	09/12/2018 02:33 PM
Duration	00:00:35
Objects Scanned	260,409
Traces Detected	8
Removal Failures	0

Settings

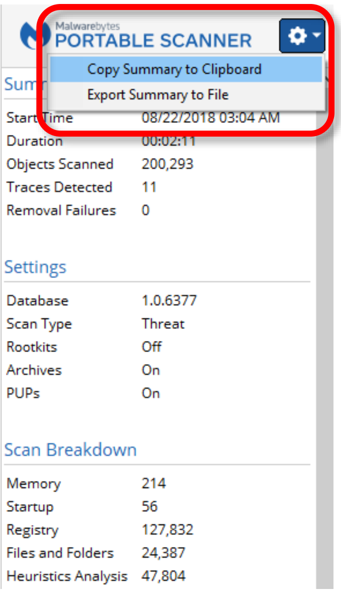
Database	1.0.6795
Scan Type	Threat
Rootkits	Off
Archives	On
PUPs	On

Scan Breakdown

Memory	73
Startup	14
Registry	111,626
Files and Folders	88,645
Heuristics Analysis	60,051

Scan status is shown in the center of the screen with a sidebar that provides selected summary information. Malware scan status may indicate remediated threats (cleaned), warnings (threats detected but not cleaned), or malware-free scans. Issue scan status may indicate system issues that are present, system issues that were repaired by *Malwarebytes Toolset*, or issue-free scans.

Each issue scan that is executed generates a log file. You may need this log file for troubleshooting purposes, or just for your records. Here's how to get that log. After running an Issue Scan, look for the Detail window associated with the scan, as shown here.



Start Time	08/22/2018 03:04 AM
Duration	00:02:11
Objects Scanned	200,293
Traces Detected	11
Removal Failures	0

Settings

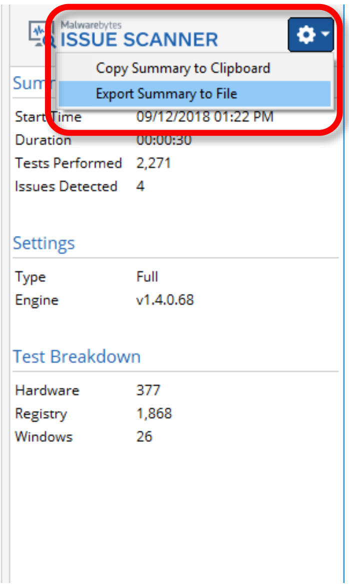
Database	1.0.6377
Scan Type	Threat
Rootkits	Off
Archives	On
PUPs	On

Scan Breakdown

Memory	214
Startup	56
Registry	127,832
Files and Folders	24,387
Heuristics Analysis	47,804

The selector in the upper right corner of each status screen allows you to copy a summary of the selected scan to your clipboard, or to a text file.

Samples of each scan type are included at end of this guide.



Start Time	09/12/2018 01:22 PM
Duration	00:00:30
Tests Performed	2,271
Issues Detected	4

Settings

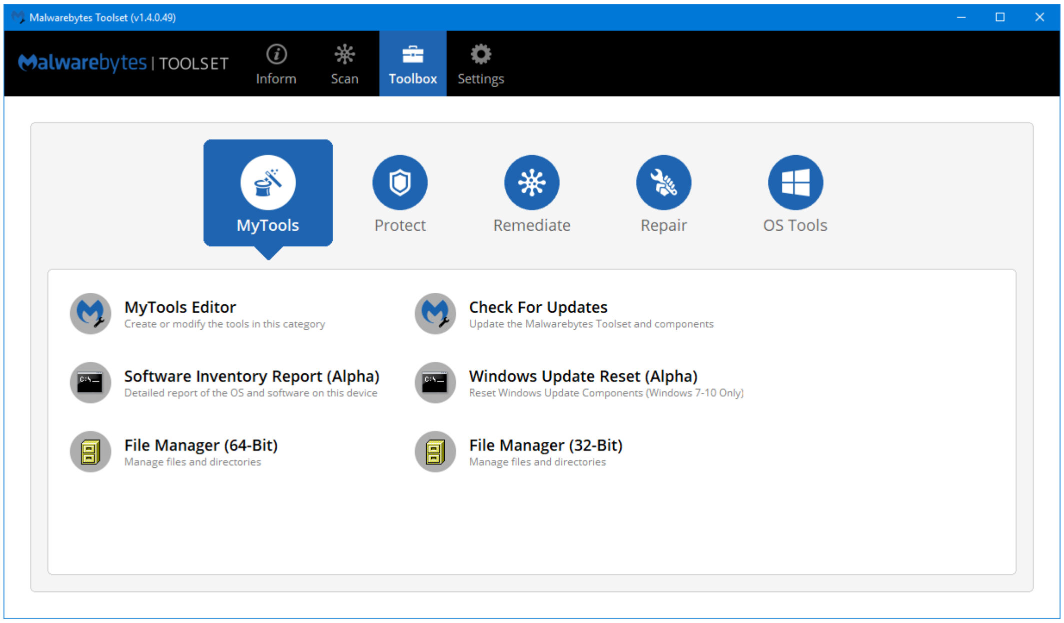
Type	Full
Engine	v1.4.0.68

Test Breakdown

Hardware	377
Registry	1,868
Windows	26

Toolbox

The **Toolbox** is a collection of tools to help you do your job better. Each part of the **Toolbox** has been carefully selected to help you evaluate and repair problem computers. We have also created an open framework which allows you to add your own tools to the Toolbox framework. Please refer to the screenshot below.



MyTools Editor
Create or modify the tools in this category

Check For Updates
Update the Malwarebytes Toolset and components

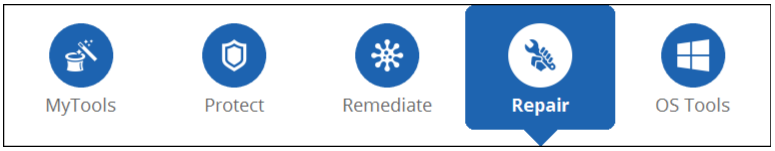
Software Inventory Report (Alpha)
Detailed report of the OS and software on this device

Windows Update Reset (Alpha)
Reset Windows Update Components (Windows 7-10 Only)

File Manager (64-Bit)
Manage files and directories

File Manager (32-Bit)
Manage files and directories

There are five sections to the **Toolbox**, which the above screenshot represents as icons. If the user interface is stretched vertically, each of the buttons also appears with a label as shown here.



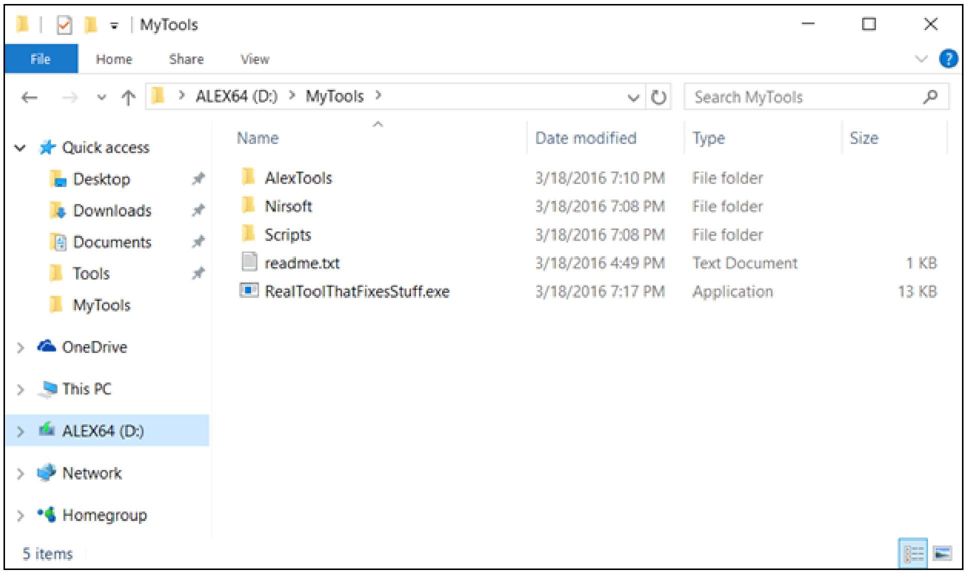
Let's look at the **Toolbox**, beginning with **MyTools**.

MyTools

MyTools provides technicians with the ability to quickly access their favorite tools. You can link to executables, execute Command Prompt/PowerShell commands, or even launch a custom batch file. The primary tool to manage **MyTools** is the *MyTools Editor*, the first item listed on the **MyTools** screen. There are several logical steps required in this section, but when configured properly, those steps will allow this to serve you well.

Staging MyTools Utilities

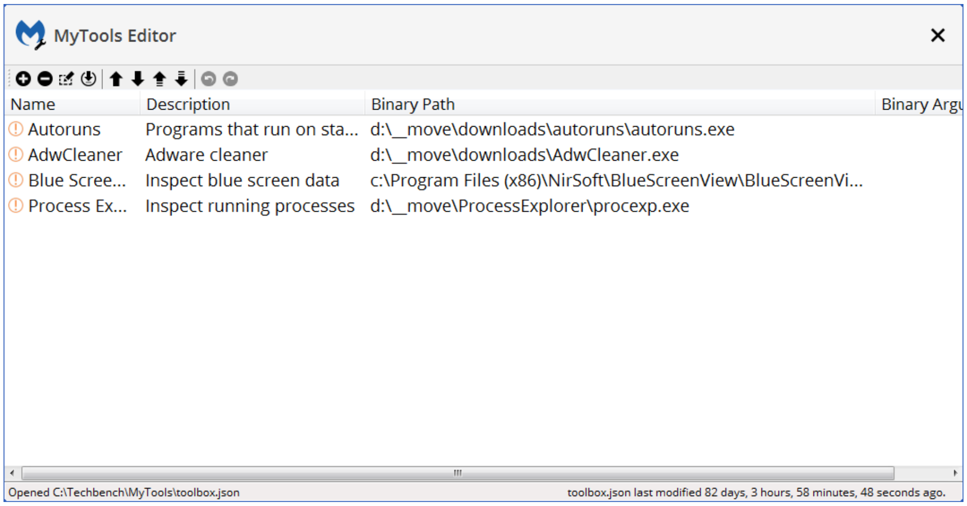
Before you get started with the *MyTools Editor*, we recommend storing your tools in the MyTools folder created when *Malwarebytes Toolset* was unzipped. This keeps the environment organized, and also makes it easier to maintain. Once you get **MyTools** built and configured, the MyTools folder can be copied to other devices *Malwarebytes Toolset* has been extracted to. Now you can distribute a customized **MyTools** configuration to your technicians on USB Flash Drives. Below is a sample configured MyTools folder.



Name	Date modified	Type	Size
AlexTools	3/18/2016 7:10 PM	File folder	
Nirsoft	3/18/2016 7:08 PM	File folder	
Scripts	3/18/2016 7:08 PM	File folder	
readme.txt	3/18/2016 4:49 PM	Text Document	1 KB
RealToolThatFixesStuff.exe	3/18/2016 7:17 PM	Application	13 KB

Managing MyTools with the MyTools Editor

Once your tools are staged, launch the *MyTools Editor*. From here you can add, remove and edit your tools. Changes are saved and implemented in real time.



Name	Description	Binary Path	Binary Argu
Autoruns	Programs that run on sta...	d:_move\downloads\autoruns\autoruns.exe	
AdwCleaner	Adware cleaner	d:_move\downloads\AdwCleaner.exe	
Blue Scree...	Inspect blue screen data	c:\Program Files (x86)\NirSoft\BlueScreenView\BlueScreenVi...	
Process Ex...	Inspect running processes	d:_move\ProcessExplorer\procexp.exe	

Opened C:\Techbench\MyTools\toolbox.json

toolbox.json last modified 82 days, 3 hours, 58 minutes, 48 seconds ago.

MyTools Editor Toolbar

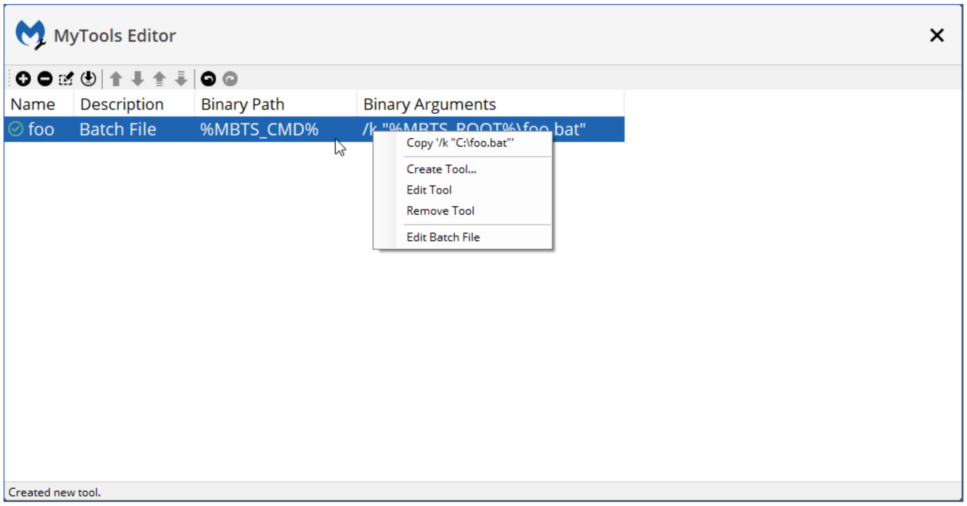
The toolbar appears directly below the *Malwarebytes Toolset* banner. It contains a number of icon buttons. To create or edit an entry, press the **+** or **Edit** icon. You can also add a new tool by clicking **<Insert>** or edit an existing tool by selecting it and pressing **<Enter>**. You can also right-click and select **Create Tool** or **Edit Tool**. The corresponding window will then be displayed. For each tool to be added, enter specifications for the tool. Below is a brief description of each field.

⊕	Add a new tool to the *Malwarebytes Toolset*. This is typically a tool which you often use in your repair work.
⊖	Remove a tool from the *Malwarebytes Toolset*.

✎	Edit criteria for an existing tool. Information on adding and editing tools is described below.
⬇	Load the Batch Import Tools window. This lets you specify a folder which contains tools to add, the specific tools, and adds them all with one click. It is preferable that the tools be moved to the MyTools directory so that any configuration or results files can be accessed without issue.
⬆	Move a selected tool higher on your priority list. You would typically do this when your repairs tend to proceed in the same logical order and your tools do not match that order.
⬇	Move a selected tool lower on your priority list.
⤒	Move a selected tool to the top of your priority list.
⤓	Move a selected tool to the bottom of your priority list.
↺	Undo whatever you just did!
↻	Redo the last action you performed.

Editing a Batch File

You can also quickly edit a batch file (CMD or BAT) using the MyTools Editor. After adding a batch file, simply right-click the item and select Edit Batch File. This will open the batch file in an instance of Notepad.exe so you can quickly manipulate it.



Name	Description	Binary Path	Binary Arguments
foo	Batch File	%MBTS_CMD%	/k "%MBTS_ROOT%\foo.bat"

Created new tool.

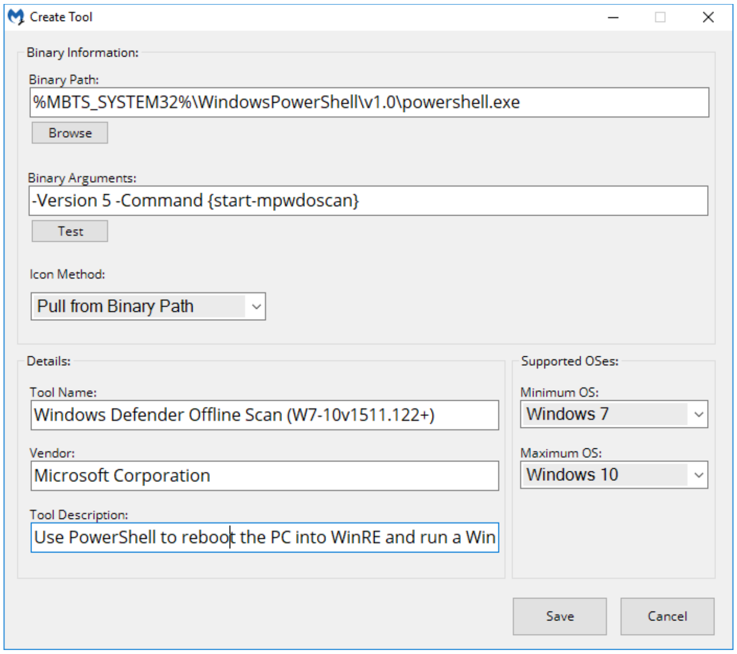
Creating or Editing a Tool Entry

To create or edit an entry, press the **+** or **Edit** icon. You can also use keyboard shortcuts (**<insert>** and **<Enter>** respectively) or right-click and select **Create Tool** or **Edit Tool**. The corresponding window will then be displayed. For each tool to be added, enter specifications for the tool. Below is a brief description of each field.

- **Binary Path –** Direct path to the tool to be added to **MyTools**. Use the **Browse** button to navigate to the tool, or type in the full path/file name. Right-click this field if you want to use special Toolset variables (described immediately after the examples provided here).

- **Binary Arguments –** Specify any special arguments or switches needed to run your tool the way you want. This field is critical for executing PowerShell *cmdlets* and performing special operations with Command Prompt-based tools. If needed, press the **Test** button to verify arguments were entered correctly.
- **Icon Method –** Select how you want **MyTools** to find the icon for the tool you are creating/editing. If an icon is stored in the tool itself, *Malwarebytes Toolset* can extract it for use here.
- **Details –** These are basic details of the tool you are creating/editing. These fields will autofill when you specify a Binary Path by pulling information from the binary itself. After selecting a binary, you can customize these fields if needed.
- **Supported OSes –** Select the oldest and newest valid Windows versions for this tool. Create for tools that can only run in certain environments. Field entries will be tested against the operating system *Malwarebytes Toolset* is being installed on. If the operating system does not match the range entered here, the tool will not appear in the tool menu. If no data is provided here, the tool will appear on the menu even if the tool is not appropriate for the operating system in question.

To help you see what's possible, here are screenshots showing examples of different types of tools and how to configure them.



Create Tool

Binary Information:

Binary Path: %MBTS_SYSTEM32%\WindowsPowerShell\v1.0\powershell.exe

Binary Arguments: -Version 5 -Command {start-mpwdoscan}

Icon Method: Pull from Binary Path

Details:

Tool Name: Windows Defender Offline Scan (W7-10v1511.122+)

Vendor: Microsoft Corporation

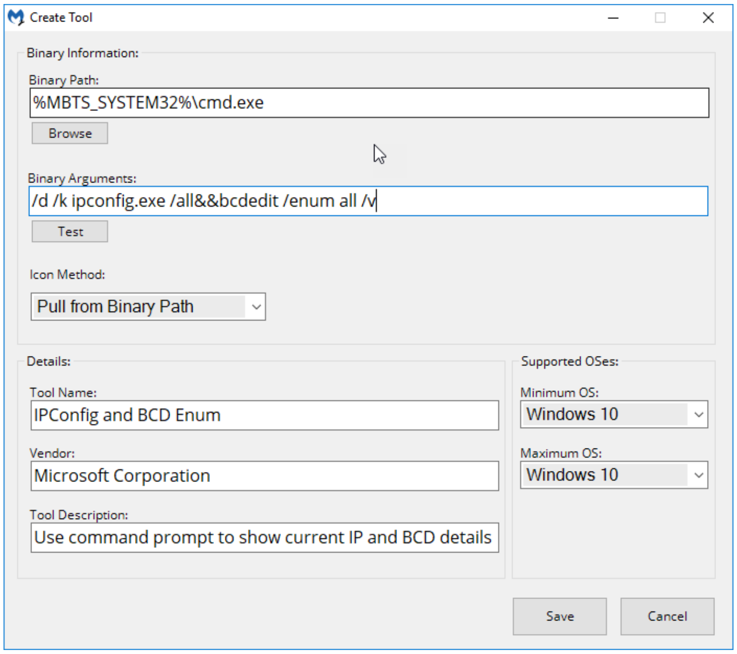
Tool Description: Use PowerShell to reboot the PC into WinRE and run a Win

Supported OSes:

Minimum OS: Windows 7

Maximum OS: Windows 10

In this example, the usage of system variables is shown. Specifications to be used during execution are also shown. In addition, this tool will only appear on the **MyTools** menu if *Malwarebytes Toolset* is running on Windows 7, Windows 8.x and Windows 10.



Binary Information:

Binary Path: %MBTS_SYSTEM32%\cmd.exe

Binary Arguments: /d /k ipconfig.exe /all&&bcdedit /enum all /v

Icon Method: Pull from Binary Path

Details:

Tool Name: IPConfig and BCD Enum

Vendor: Microsoft Corporation

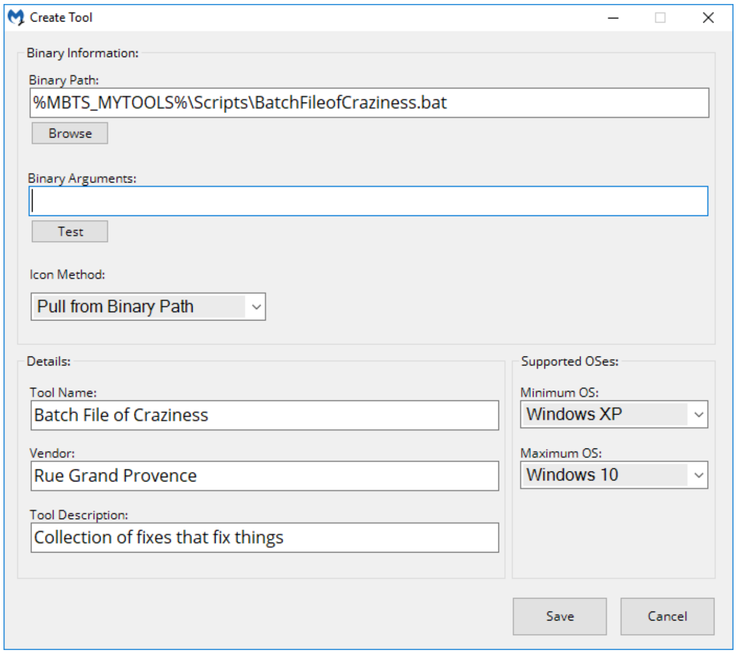
Tool Description: Use command prompt to show current IP and BCD details

Supported OSes:

Minimum OS: Windows 10

Maximum OS: Windows 10

The above example demonstrates the usage of both system variables (Binary Path) as well as specifications (Binary Arguments) to be utilized during execution of the tool. Here, Supported OSes will allow this tool to appear on the **MyTools** menu when *Malwarebytes Toolset* is running on a Windows 10 computer.



Binary Information:

Binary Path: %MBTS_MYTOOLS%\Scripts\BatchFileofCraziness.bat

Binary Arguments:

Icon Method: Pull from Binary Path

Details:

Tool Name: Batch File of Craziness

Vendor: Rue Grand Provence

Tool Description: Collection of fixes that fix things

Supported OSes:

Minimum OS: Windows XP

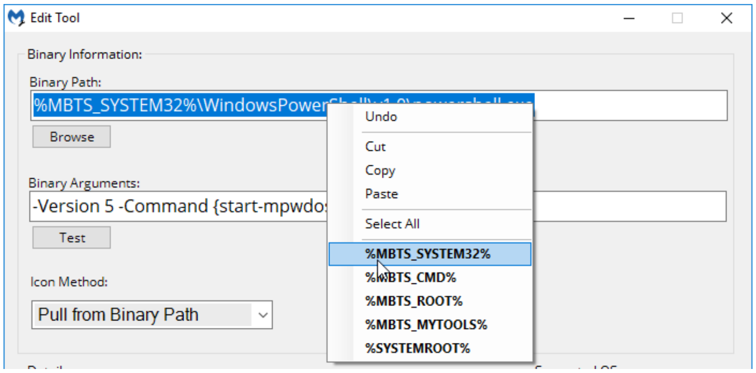
Maximum OS: Windows 10

Here, a handcrafted batch file will be used, which presumably contains references to a number of executables or command line entries. No binary arguments are specified, and a generic icon will be shown for the tool.

Using Toolset Variables in MyTools

When specifying a Binary Path or Binary Arguments for any tool, you can right-click the field to add special Toolset Variables. This not only simplifies entry of long directory paths, but also helps to ensure your tools can launch across multiple computers – especially if you are storing and running *Malwarebytes Toolset* from a USB Flash Drive. The following variables have been defined.

- **%MBTS_SYSTEM32% -** The \Windows\SysNative directory of the host operating system
- **%MBTS_CMD% -** Launches Command Prompt from the default location based on the host operating system
- **%MBTS_ROOT% -** The root directory *Malwarebytes Toolset* itself is running from.
- **%MBTS_MYTOOLS% -** The *MyTools* subdirectory that is in the root directory *Malwarebytes Toolset* itself is running from
- **%SYSTEMROOT% -** The root directory of the host operating system



Binary Information:

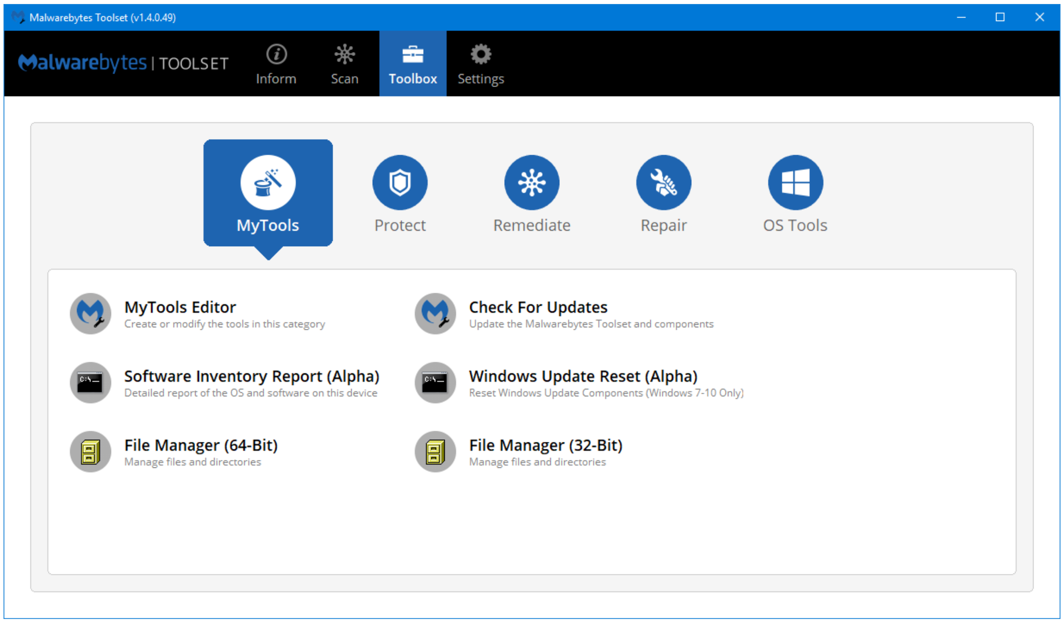
Binary Path: %MBTS_SYSTEM32%\WindowsPower

Binary Arguments: -Version 5 -Command {start-mpwdo

Icon Method: Pull from Binary Path

Editing Complete...What Now?

Once you have added all of the tools you wish to use (or made changes when required), close the *MyTools Editor*. The *Malwarebytes Toolset* user interface will appear similar to what is shown below. Depending on the width of the interface displayed on your screen, you may see tools arranged as one long column, or in two columns (as shown here). Note that all tools shown here are ones that were just entered.



MyTools Editor
Create or modify the tools in this category

Check For Updates
Update the Malwarebytes Toolset and components

Software Inventory Report (Alpha)
Detailed report of the OS and software on this device

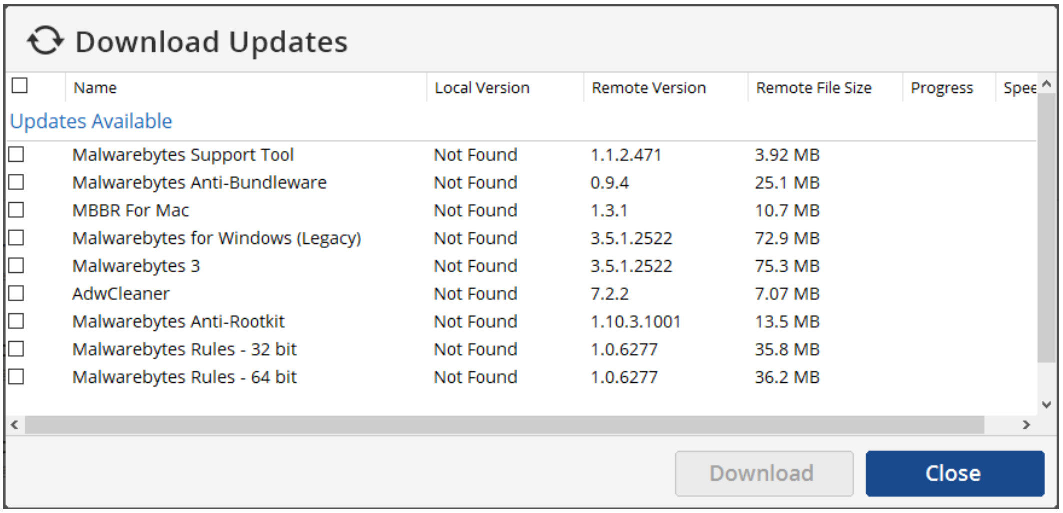
Windows Update Reset (Alpha)
Reset Windows Update Components (Windows 7-10 Only)

File Manager (64-Bit)
Manage files and directories

File Manager (32-Bit)
Manage files and directories

Check for Updates

This option enables the *Malwarebytes Toolset* to look for pertinent updates which may be available. This includes updates to the *Toolset* itself as well as all *Malwarebytes* utilities which are made available through the *Toolset*. Updates will appear on the list (as shown below) for utilities which have not yet been downloaded, or for utilities which updates are available for. If a program has been downloaded and is up to date, it will not appear on the list.


Download Updates

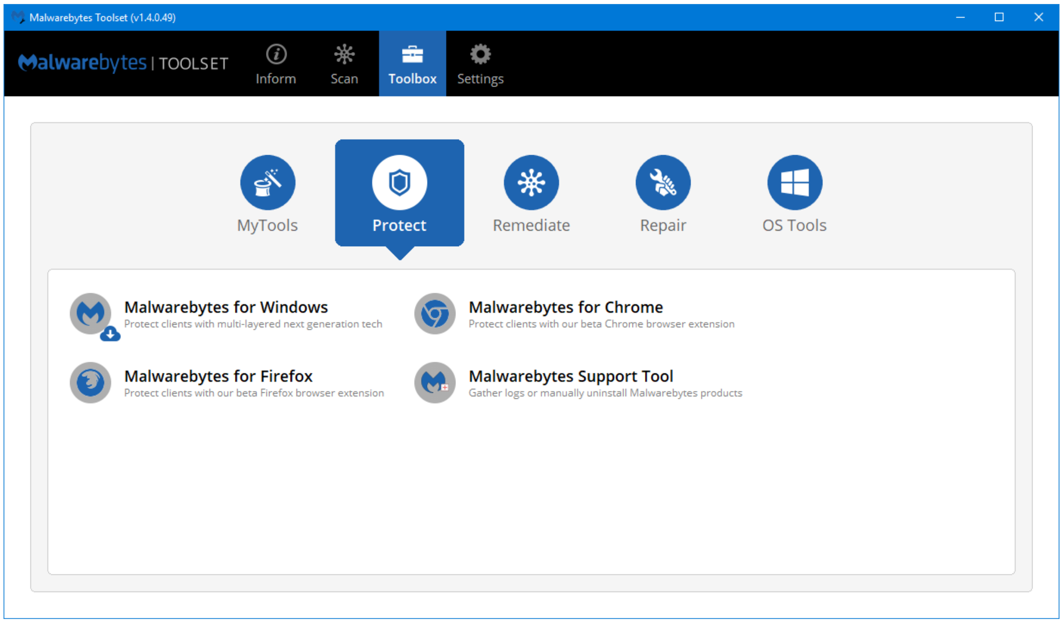
□	Name	Local Version	Remote Version	Remote File Size	Progress	Spee
Updates Available						
□	Malwarebytes Support Tool	Not Found	1.1.2.471	3.92 MB		
□	Malwarebytes Anti-Bundleware	Not Found	0.9.4	25.1 MB		
□	MBBR For Mac	Not Found	1.3.1	10.7 MB		
□	Malwarebytes for Windows (Legacy)	Not Found	3.5.1.2522	72.9 MB		
□	Malwarebytes 3	Not Found	3.5.1.2522	75.3 MB		
□	AdwCleaner	Not Found	7.2.2	7.07 MB		
□	Malwarebytes Anti-Rootkit	Not Found	1.10.3.1001	13.5 MB		
□	Malwarebytes Rules - 32 bit	Not Found	1.0.6277	35.8 MB		
□	Malwarebytes Rules - 64 bit	Not Found	1.0.6277	36.2 MB		

Select updates you wish to download and click **Download**. The window will update to show status of the download, and will inform you of final download status. When the download is complete, click **Close**.

In the next section of this guide, you will notice small clouds at the bottom right of two utilities, and the absence of a cloud on the MC-Check icon. That indicates that two utilities have updates available, while the third does not. That standard is used throughout the Toolbox section of this program.

Protect

This area provides easy access to install our flagship product – *Malwarebytes for Windows* – as well as utilities that are often used in conjunction with *Malwarebytes for Windows*.



Malwarebytes for Windows
Protect clients with multi-layered next generation tech

Malwarebytes for Chrome
Protect clients with our beta Chrome browser extension

Malwarebytes for Firefox
Protect clients with our beta Firefox browser extension

Malwarebytes Support Tool
Gather logs or manually uninstall Malwarebytes products

Malwarebytes for Windows

This option installs the latest version of *Malwarebytes for Windows* on the target computer, using specifications defined by the user. While we encourage users to install *Malwarebytes Premium* version to take advantage of the real-time protection it offers, the free version will allow the computer owner to run scans at will. If *Malwarebytes for Windows* has not been previously downloaded (or an updated version exists), it will be downloaded and then executed.

Malwarebytes for Chrome

This option will open the default web browser of the target computer and go to the Malwarebytes for Chrome browser extension page at the Chrome Web Store. This will allow you to add proactive protection at the web browser level to protect a system from malware, scams, clickbait, and annoying ads.

Malwarebytes for Firefox

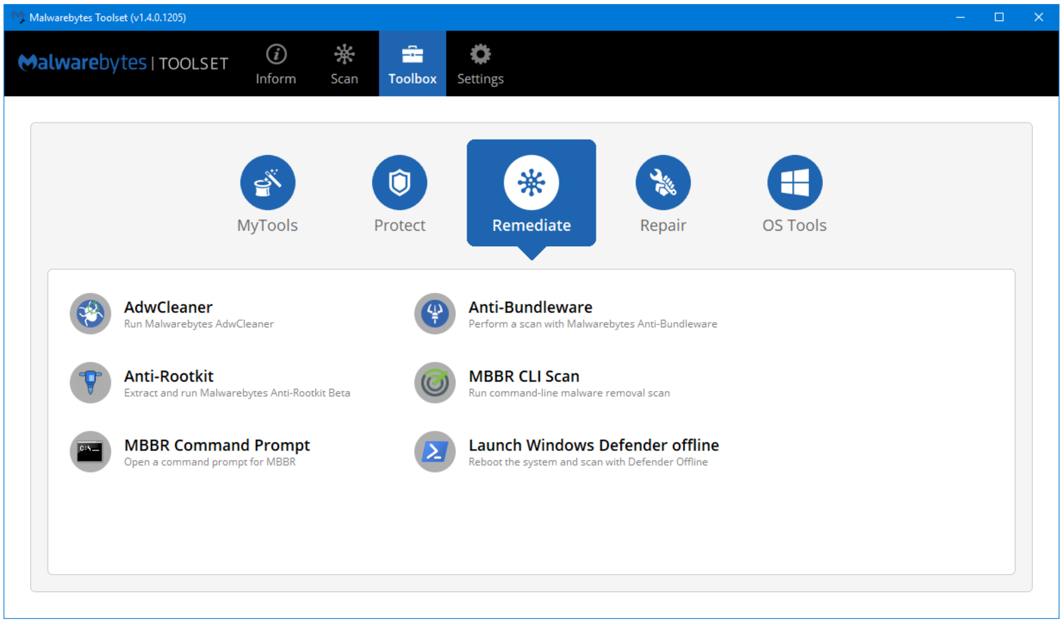
This option will open the default web browser of the target computer and go to the Malwarebytes for Firefox browser extension page at the Firefox Add-ons site. This will allow you to add proactive protection at the web browser level to protect a system from malware, scams, clickbait, and annoying ads.

Malwarebytes Support Tool

This utility allows you to manually remove Malwarebytes products and potential leftovers on a computer. It also helps in gathering in-depth technical logs of a system and installed Malwarebytes products to help troubleshoot issues with our products. See the Malwarebytes Support Tool FAQ (https://support.malwarebytes.com/hc/en-us/articles/360038524914) for more details on using this utility.

Remediate

This option provides several Malwarebytes programs to assist in the remediation and cleanup of a computer. You may choose to limit your toolset to the tools you have added in the **MyTools** section. That is your choice, but we also offer these tools to you all in one place for ease of use.


Malwarebytes Toolset (v1.4.0.1205)
Malwarebytes | TOOLSET
Inform
Scan
Toolbox
Settings
MyTools
Protect
Remediate
Repair
OS Tools
AdwCleaner
Run Malwarebytes AdwCleaner
Anti-Bundleware
Perform a scan with Malwarebytes Anti-Bundleware
Anti-Rootkit
Extract and run Malwarebytes Anti-Rootkit Beta
MBBR CLI Scan
Run command-line malware removal scan
MBBR Command Prompt
Open a command prompt for MBBR
Launch Windows Defender offline
Reboot the system and scan with Defender Offline

Here is more information about each of these tools.

Malwarebytes Anti-Bundleware

Malwarebytes Anti-Bundleware is a program designed to detect and remove bundleware which may have been pre-installed on your system or automatically installed with another piece of software. More details about this program can be found on our forums: https://forums.malwarebytes.com/forum/233-malwarebytes-anti-bundleware/.

Malwarebytes Anti-Rootkit

Malwarebytes Anti-Rootkit is a program designed to detect and repair rootkits which may have been placed on your disk drive via a malware attack. This program is a perpetual beta product, meaning that it is updated only when there is a specific need.

AdwCleaner

This is one of the most frequently downloaded tools for removal of potentially unwanted programs (PUPs), toolbars and adware. Addition of AdwCleaner technology to your repertoire helps to provide even more effectiveness to the services you provide. If *AdwCleaner* has not been previously downloaded (or an updated version exists), it will be downloaded and then executed.

► ***AdwCleaner* includes the technology of the Junkware Removal Tool.**

MBBR CLI Scan

This option performs a Threat Scan on the computer from the command line using Malwarebytes Breach Remediation. There is no provision for customization of the arguments. If the computer does not have .NET 4.0 installed (or if it has been rendered unusable), this is the only method available for portable malware scanning.

► **If malware is detected, you may be prompted to reboot the computer. Please plan accordingly.**

MBBR Command Prompt

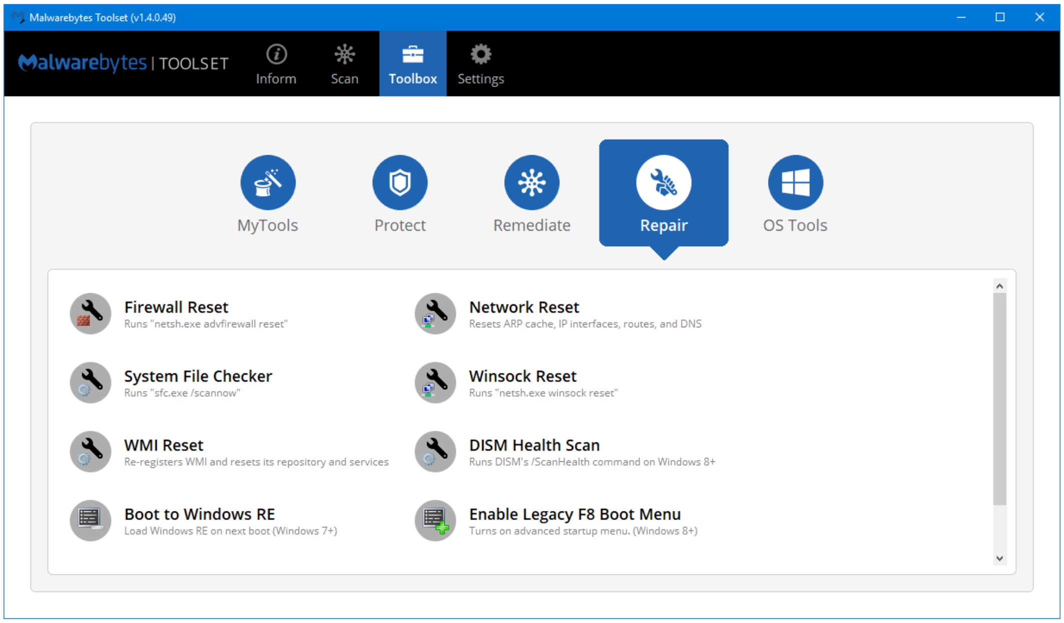
This option will open a Command Prompt instance with focus on the directory where MBBRv2 is stored so you can run Malwarebytes Breach Remediation however you see fit. It will prompt to register and update definitions for MBBRv2 for you to make things as easy as possible.

Launch Windows Defender Offline

This option is available for Windows 10 users **only**. It causes the system to reboot, then performs an offline scan using Microsoft Windows Defender.

Repair

This section provides a number of tools to fix problems that often occur as a result of malware attacks. A proficient technician can inspect each component and manually correct deficient areas, or use these tools to quickly and efficiently restore these system settings. A few of these tools are not available for computers running operating systems older than Windows 8. This will also be spelled out for the affected tools. Let's begin by looking at a screenshot of the Repair section of the Toolbox.



Firewall Reset
Runs "netsh.exe advfirewall reset"

Network Reset
Resets ARP cache, IP interfaces, routes, and DNS

System File Checker
Runs "sfc.exe /scannow"

Winsock Reset
Runs "netsh.exe winsock reset"

WMI Reset
Re-registers WMI and resets its repository and services

DISM Health Scan
Runs DISM's /ScanHealth command on Windows 8+

Boot to Windows RE
Load Windows RE on next boot (Windows 7+)

Enable Legacy F8 Boot Menu
Turns on advanced startup menu. (Windows 8+)

Firewall Reset

Computers are often infected by malware which manipulates firewall settings, thus opening the computer to access from the outside world. This command resets the firewall to the default policy. When Group Policy is used, all firewall settings are turned off and Group Policy settings pertaining to the firewall are set to *not configured*.

Network Reset

Many connectivity issues are due to problems with configuration of the various networking components on the computer. Sometimes this is due to malware, and sometimes not. This option resets most of those components to initial values. As a result, subsequent networking commands encounter very slight delays as these initial values are replaced by true operational values. Please note that this option does not accomplish the same goals as a Winsock Reset, and when required, should be performed before use of a Winsock Reset is considered.

System File Checker

This option executes the Windows System File Checker utility program (**`sfc.exe`**). This program scans Windows system files, and attempts to repair any corrupted files found during the scan. This is not a replacement for the **`chkdsk`** utility.

Winsock Reset

If the computer is exhibiting strange connectivity issues that have not been corrected by other diagnostic means, you may need to reset the winsock catalog. This catalog is used for all Internet connectivity, and is a favorite target of malware. Unless the computer uses customized networking parameters, a reset would not have negative results.

WMI Reset

Windows Management Instrumentation (WMI) is infrastructure built into Windows for managing devices, applications, data and operating system components. It is also used to share management data and operations with other operating system components. This reset will rebuild and register the core components of Windows that allow WMI to function.

DISM Health Scan

Deployment Image Service and Management Tool (DISM) is used on computers running Windows 8 and above, to check the computer's component store against its own payload. Any files found to be corrupted are replaced by files downloaded files through the Windows Update process. This option is **not** available on Windows XP, Windows 7 or Windows Vista.

Boot to Windows RE

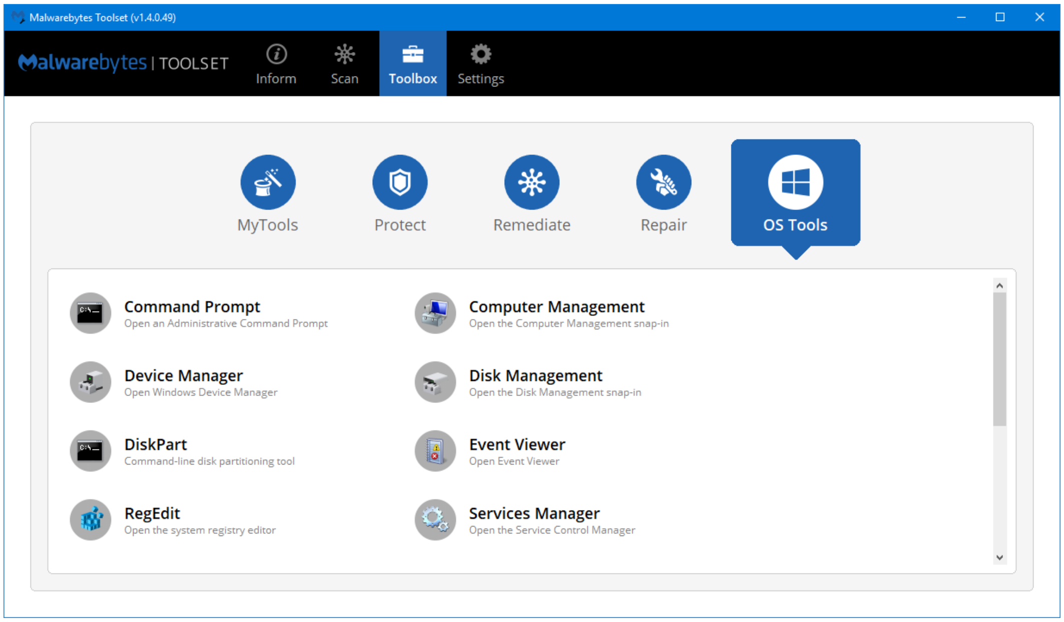
The Windows Recovery Environment (Windows RE) is a bootable offline Windows PE based environment to help one manually repair or restore their operating system using tools like System Restore, Refresh/Reset (Windows 8+), Command Prompt, and much more. Windows RE is included by default starting with Windows 7 and can be a powerful tool for technicians. This option allows a technician to set the assigned Windows RE image of the OS to load on next boot. This option is **not** available on Windows XP or Windows Vista.

Enable/Disable Legacy F8 Boot Menu

In Windows 8.x and Windows 10, the boot loader was modified to speed up the time required to boot the computer. As a result, the Safe Mode option (F8) was removed. This feature still exists, but only through a setting in the Windows registry. This option allows the technician to enable/disable the F8 Boot Menu using a Windows utility that modifies the registry key. This option is **not** available on Windows XP, Windows Vista or Windows 7.

OS Tools

This tab provides a collection of important system-level tools which are available in modern Windows operating systems. While these tools will not detect malware on a system, they may detect the aftereffects of malware. A screenshot is shown here.



Command Prompt
Open an Administrative Command Prompt

Computer Management
Open the Computer Management snap-in

Device Manager
Open Windows Device Manager

Disk Management
Open the Disk Management snap-in

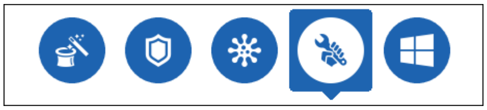
DiskPart
Command-line disk partitioning tool

Event Viewer
Open Event Viewer

RegEdit
Open the system registry editor

Services Manager
Open the Service Control Manager

Please note the shaded area of the main screen area, which shows five labeled icons. This is the view you will see normally. When the screen is compressed vertically, it appears as shown below.



As with all system-level tools, significant damage may easily result from inappropriate usage. If you are not sure about changing a system setting, please research that setting before making a change from which there may be no cure.

Command Prompt

This option opens a Windows command prompt (cmd.exe), in Administrator mode. You may navigate to any directory on any mounted drive and perform command line operations.

Computer Management

This option launches the Computer Management snap-in of the Microsoft Management Console (`mmc.exe`). Many system parameters may be inspected here. Event Viewer and Device Manager are available within this option, as well as being accessible by their own program option.

Device Manager

This option launches the Device Manager snap-in of the Microsoft Management Console (`mmc.exe`). Entries for each installed hardware device may be inspected, along with the resources those devices use. Failing or misconfigured devices will have a warning indicator displayed to alert the user. This option is available as a discrete menu selection, and as a selectable option in Computer Management.

Disk Management

This option launches an analysis of each disk and disk partition in the storage subsystem. Drives which are not assigned drive letters (unused areas, recovery partitions and disk used for secondary operating systems) are all shown, as are CD/DVD/Blu-ray and virtual drives. This option is available as a discrete menu selection, and as a selectable option in Computer Management.

DiskPart

This tool allows the technician to create new disk partitions, or to delete or modify existing disk partitions. It is a replacement for Microsoft's legacy program, `fdisk`. This program offers a number of configuration options. Please refer to the following page for more information on this program.

https://technet.microsoft.com/en-us/library/bb490893.aspx

Event Viewer

This option launches the Windows Event Viewer snap-in of the Microsoft Management Console (`mmc.exe`). All system events may be inspected here.

RegEdit

This option opens the Windows Registry Editor (`regedit.exe`). Unless you are well versed in working with the Windows registry, you should make a backup copy of the registry before proceeding.

Services Manager

This option opens the Windows Service Control Manager snap-in of the Microsoft Management Console (`mmc.exe`). This tab shows each system service, its operating status, when the service starts, and under which user's authority.

Settings

This option provides access to system settings on computers using Windows 8, 8.1 and 10 operating systems. This option will not appear on computers running earlier versions of the Windows operating system.

Task Manager

This option opens the Windows Task Manager (`taskmgr.exe`), allowing inspection of running applications, processes and services, each on their own tabs. CPU usage and memory usage as well as networking usage are also available for inspection.

Windows Explorer/File Explorer

This option opens Windows Explorer (Windows 7 and earlier) or File Explorer (Windows 8 and newer), allowing navigation from one drive or directory to another. This option will **not** provide option to restricted operating system directories.

Windows Memory Diagnostic

This option launches a delayed diagnostic test of all RAM memory installed in the computer, using Microsoft's `mdsched.exe` diagnostic. This requires that you must reboot the computer after selecting this option to allow the test to run. **Please note** that you cannot use the computer for any other purpose while the test is running, and this test may take several minutes to complete.

Progress will be displayed on the screen, and the computer will reboot when the test is complete. Depending on the operating system in use, you may be able to evaluate test results on screen. If you are unable to view test results, they are available in the Windows Event Viewer in the System Log section.

Windows PowerShell

This option opens a Windows PowerShell command prompt (`powershell.exe`). You may perform system-level commands, which include many commands that have not been available in the older Windows command prompt (cmd.exe). **Please note** that this option is visible only for operating systems that will support it (Windows 7 and newer).

Windows Store App Updates

This option provides access to information on application updates on computers using Windows 8, 8.1 and 10 operating systems. Version numbers and dates that applications were last updated are shown here. This option will not appear on computers running earlier versions of the Windows operating system.

Windows Troubleshooters

This option provides access to the troubleshooting tools provided by Microsoft for users of Windows 7 and newer operating systems. This option will not appear on versions of Windows older than Windows 7.

Windows Update

This option opens the Windows Update option of the Control Panel. You may check for new updates, install or roll back updates. If updates are controlled by a system administrator (typical in a corporate environment), this option cannot override that authority.

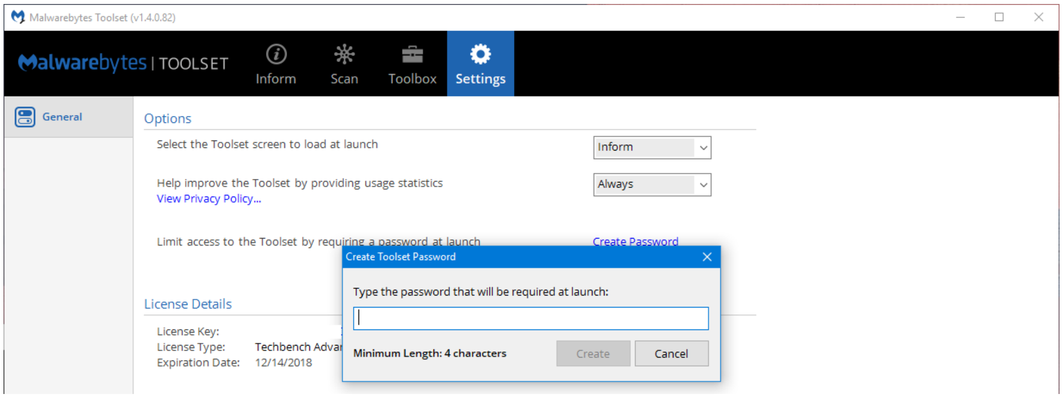
Settings

Malwarebytes Toolset includes an area to manage general settings of the application, manage your license, and set a Startup Password. The following options are available under Settings.

Options & Startup Password

This section contains options to help customize your experience with the Toolset. They are:

- **Select the Toolset screen to load at launch**: This sets which screen/component of the Toolset loads when you launch it. Available options are:
  - Inform (Default)
  - Scan
  - Toolbox
  - Settings
- **Help improve the Toolset by providing usage statistics**: This configures the telemetry capabilities of the Toolset to help us improve its capabilities. Available options are:
  - Always (default)
  - Never
  - For more details on the data we collect with our products, see our Privacy Policy.
- **Limit access to the Toolset by requiring a password at launch:** This allows you to set a Startup Password to limit unauthorized access to the Toolset.
  - To enable this feature, click the **Create Password** link and you will be presented with a window to enter a custom password with a minimum of four (4) characters.



Malwarebytes Toolset (v1.4.0.82)

Options

Select the Toolset screen to load at launch: Inform

Help improve the Toolset by providing usage statistics: Always
View Privacy Policy...

Limit access to the Toolset by requiring a password at launch: Create Password

Create Toolset Password

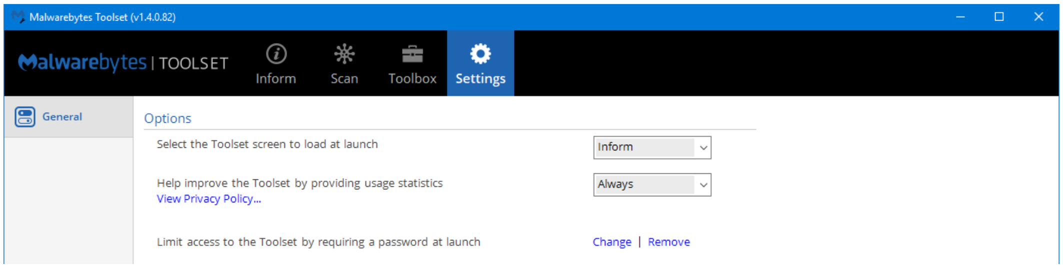
Type the password that will be required at launch:

Minimum Length: 4 characters

License Details

License Key:
License Type: Techbench Advai
Expiration Date: 12/14/2018

  - Once a Startup Password is enabled, you can change it by clicking **Change** or remove it by clicking **Remove**.



Malwarebytes Toolset (v1.4.0.82)

Options

Select the Toolset screen to load at launch: Inform

Help improve the Toolset by providing usage statistics: Always
View Privacy Policy...

Limit access to the Toolset by requiring a password at launch: Change | Remove

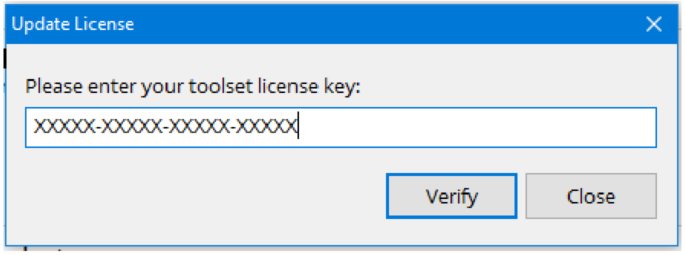
  - If you have forgotten your Startup Password, you can recover access by doing the following:

1. Delete the Toolset license file at “\Malwarebytes\MBTS\Data\Configuration\mbts-license.dat”
2. Relaunch the Toolset
3. Enter your Toolset license key and click Verify

License Details

This section allows you to view your license key and change it if necessary.

- **License Key**: This shows the current license key being used. Click on it to be prompted with a window to change it



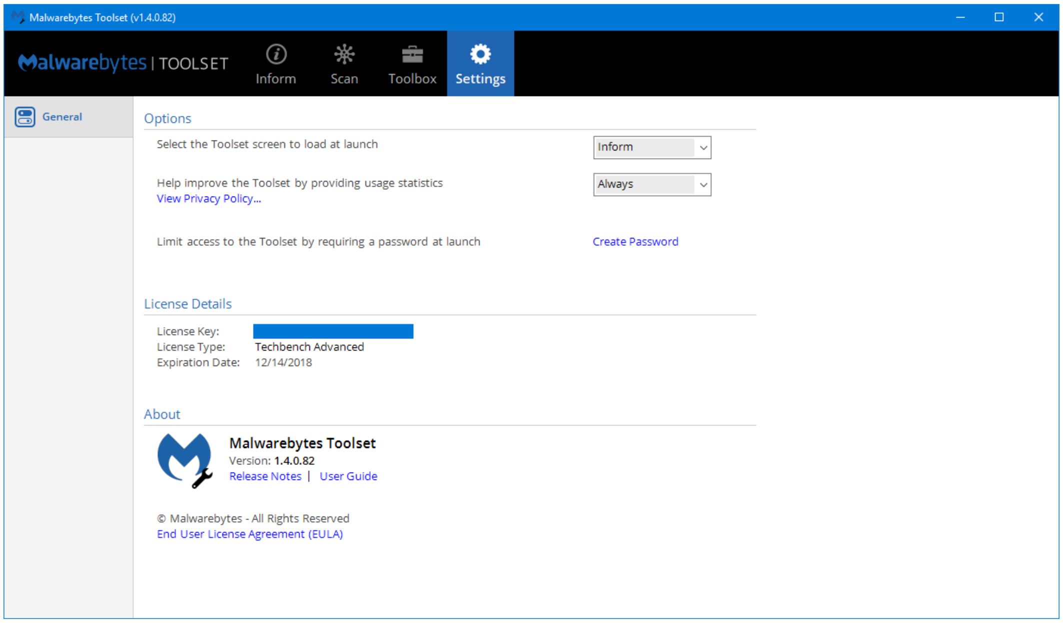
Please enter your toolset license key:

XXXXX-XXXXX-XXXXX-XXXXX

- **License Type**: This displays the current type of license being used.
- **Expiration Date**: The current date your *Malwarebytes Toolset* license will expire. For license or renewal questions, contact techbench@malwarebytes.com

About

This section shows version details of *Malwarebytes Toolset* with links to release notes, user guide, and EULA.



Options

Select the Toolset screen to load at launch: Inform

Help improve the Toolset by providing usage statistics: Always
View Privacy Policy...

Limit access to the Toolset by requiring a password at launch: Create Password

License Details

License Key: [redacted]
License Type: Techbench Advanced
Expiration Date: 12/14/2018

About

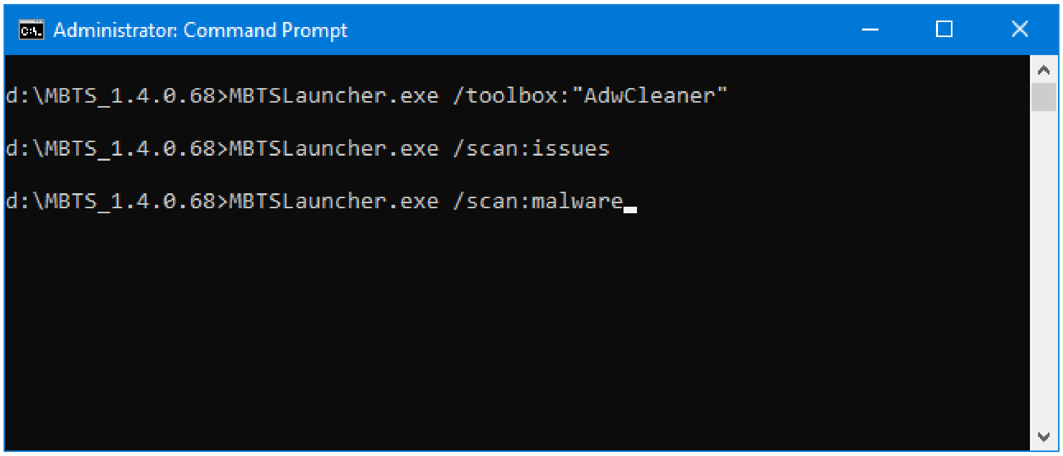
Malwarebytes Toolset
Version: **1.4.0.82**
Release Notes | User Guide

© Malwarebytes - All Rights Reserved
End User License Agreement (EULA)

Command Line Options

The *Malwarebytes Toolset* provides Command Line options to utilize some components quickly for automation and/or scripting purposes. These options can be passed to **MBTSLauncher.exe** or **MBTS.exe**. Below is a list of those options with examples.

- **/password:"Your Startup Password"** - Suppress prompt for your Startup Password.
- **/scan:inform /LogFile:"Path to file"** - Silently runs an Inform operation and outputs results in plain text to the file specified.
    - If **/LogFile** is not specified, then the exported text file is saved to the following location: %UserProfile%\Desktop\Inform_%COMPUTERNAME%_%DATE&TIME%.txt
    - If only a file name is specified for **/LogFile** (e.g. "Inform Log File.log"), then the specified file will be saved to %MBTS_ROOT% (aka the directory where MBTSLauncher.exe is stored).
    - **NOTE:** MBTS.exe is not a console app. No output will be sent to the console window while the export is occurring.
- **/scan:malware** - Scans for malware with the Malwarebytes Portable Scanner using the current Default Scan settings. These settings can be changed using the MBTS.exe GUI (Scan ► Settings icon ► Edit Default Scan).
- **/scan:issues** – Scans for issues with the Malwarebytes Issue Scanner.
- **/repair:network** – Performs a Network Reset.
- **/repair:wmi** – Performs a WMI Reset.
- **/toolbox:"Name of Tool"** – Launches the specified tool in quotes from the Toolbox or MyTools.
- /**LogLevel:<0-5>** – Launches the *Malwarebytes Toolset* with a specified logging level output for the "DebugLogging.txt" file. This is used for troubleshooting the Malwarebytes Portable Scanner. The default log level is 1 (ERRORS) and is used if no log level is specified. The following is a definition of each log level:
    - 0 - none
    - 1 – Events marked as Errors only are logged
    - 2 – Events marked as Errors and Warnings are logged
    - 3 – Events marked as Errors, Warnings, and Info are logged
    - 4 – Events marked as Errors, Warnings, Info, and Debug are logged
    - 5 – Events marked as Errors, Warnings, Info, Debug, and Trace are logged
    - The DebugLogging.txt file is stored in the following locations depending on the architecture of the operating system:
        - 64-Bit (x64) - Malwarebytes\MBTS\x64\DebugLogging.txt
        - 32-Bit (x86) - Malwarebytes\MBTS\DebugLogging.txt



```
d:\MBTS_1.4.0.68>MBTSLauncher.exe /toolbox:"AdwCleaner"

d:\MBTS_1.4.0.68>MBTSLauncher.exe /scan:issues

d:\MBTS_1.4.0.68>MBTSLauncher.exe /scan:malware_
```

Reports and Scan Logs

Malwarebytes Toolset can capture and export the results of scans –Inform, Network Devices Scan, Issue Scanner, and Malwarebytes Portable Scanner– to your clipboard, to text files, and (in some cases) to specialized files on the system itself. This allows you to export results to wherever you need them for documentation, reporting, troubleshooting, or other similar needs.

Inform Export Log

This log is an optional export from Inform. It's designed to provide users a way to export all the rich technical information that Inform gathers on the operating system and device. This can be very helpful for service documentation, reporting, or other similar use cases. To create an Inform Export Log from within *Malwarebytes Toolset*:

1. Go to **Inform** and select **Actions**
2. Select the desired operation:
    a. Export to Clipboard – This will export all detected devices and details in plain text to the clipboard
    b. Export to Text File – This will export all detected devices and details to a text file

Malwarebytes Issue Scanner Reports and Summary Log

The Malwarebytes Issue Scanner saves a detailed report of each scan and repair operation on the local system via Scan History. You can export a summary-based log of any issue scan by doing the following:

1. Go to **Scan** and click the **Scan History** icon (looks like a calendar) in the Malwarebytes Portable Scanner section
2. Select the scan report you want to load and click **View**
3. Click the gear icon near the top of the summary pane and select the desired operation:
    a. Copy Summary to Clipboard – This will export a summary of the scan, issues found, and issues repaired in plain text to the clipboard
    b. Export Summary to Text File – This will export a summary of the scan, issues found, and issues repaired to a text file

Note: You can also export a summary report at the Scan Results and Repair Results phases of a scan operation.

You can view full technical details of a Malwarebytes Issue Scanner operation from within *Malwarebytes Toolset* by clicking the **Scan History** icon (looks like a calendar) under the Scan component, then selecting a scan report and clicking **View**. This allows you to view the full Scan Report and Repair Report details that were presented during the original scan operation.

Malwarebytes Portable Scanner Reports and Summary Log

The Malwarebytes Portable Scanner saves a detailed report of each scan and removal operation on the local system. You can export a summary-based log of any malware scan by doing the following:

1. Go to **Scan** and click the **Scan History** icon (looks like a calendar) in the Malwarebytes Portable Scanner section
2. Select the scan report you want to load and click **View**
3. Click the gear icon near the top of the summary pane and select the desired operation:
    a. Copy Summary to Clipboard – This will export a summary of the scan and malware removed in plain text to the clipboard
    b. Export Summary to Text File – This will export a summary of the scan and malware removed to a text file

Note: You can also export a summary report at the Scan Results and Repair Results phases of a scan operation.

You can view full technical details of a Malwarebytes Portable Scanner operation from within *Malwarebytes Toolset* by clicking the Scan History icon (looks like a calendar) under the Scan Component then selecting a scan report and clicking **View**. This allows you to view the full Scan Report and Repair Report details that were presented during the original scan operation.

Alternatively, you can also get a detailed scan results JSON file if needed. These are stored in the following location:

- %ProgramData%\Malwarebytes\Malwarebytes Toolset\MalwareScanner_Client\ScanResults\GUID.json – scan results files in JSON format produced by the Malwarebytes Portable Scanner

Network Devices Scan Log

This log is an optional export from the Network Devices Scanner. It's designed to provide users with an ability to produce a network site survey or inventory of local network devices. Please note that the fields of this report can be customized before exporting. To create a Network Devices Scan Log from within the *Malwarebytes Toolset*:

1. Go to Inform and select Network
2. Click Start Scan under the Network Discovery tile
3. Wait for the Network Devices Scan to finish
4. Click Export and select the desired operation:
    a. Copy to Clipboard – This will export all detected devices and details in plain text to the clipboard
    b. Export to Text File – This will export all detected devices and details to a text file
    c. Export to CSV – This will export the summary of detected devices to a CSV file

Other Log Files

Additional log files are created for specific components that can help with customized reporting needs and troubleshooting. Below is a list of these with a brief description of their contents.

- %ProgramData%\Malwarebytes\Malwarebytes Toolset\Logs\*.mbts – Scan History data files for the Malwarebytes Portable Scanner and Malwarebytes Issue Scanner
- %ProgramData%\Malwarebytes\Malwarebytes Toolset\MalwareScanner_Client\ScanResults\GUID.json – scan results files in JSON format produced by the Malwarebytes Portable Scanner
- \Malwarebytes\MBTS\DebugLogging.txt – debug log file for the Malwarebytes Portable Scanner (32-bit)
- \Malwarebytes\MBTS\x64\DebugLogging.txt – debug log file for the Malwarebytes Portable Scanner (64-bit)
- \Malwarebytes\MBBRv3\x64\Logs\MBBR-ERROUT.txt –error and debug log files for Malwarebytes Breach Remediation CLI v3 64-Bit
- \Malwarebytes\MBBRv3\x86\Logs\MBBR-ERROUT.txt –error and debug log files for Malwarebytes Breach Remediation CLI v3 32-Bit
- \Malwarebytes\MBBRv2\Logs\MBBR-ERROUT.txt – the error and debug log file for Malwarebytes Breach Remediation CLI v2

Additional Tools

Malwarebytes Toolset has additional standalone tools available to users either in a dedicated directory with the Toolset package or as a separate download. Below are the current additional tools available.

Malwarebytes Breach Remediation for Windows

Malwarebytes Breach Remediation for Windows is a portable command-line version of our Malwarebytes technology designed to facilitate malware remediation on Windows and Windows Server. This utility can be scripted to provide advanced usage and automation which may be needed for certain environments.

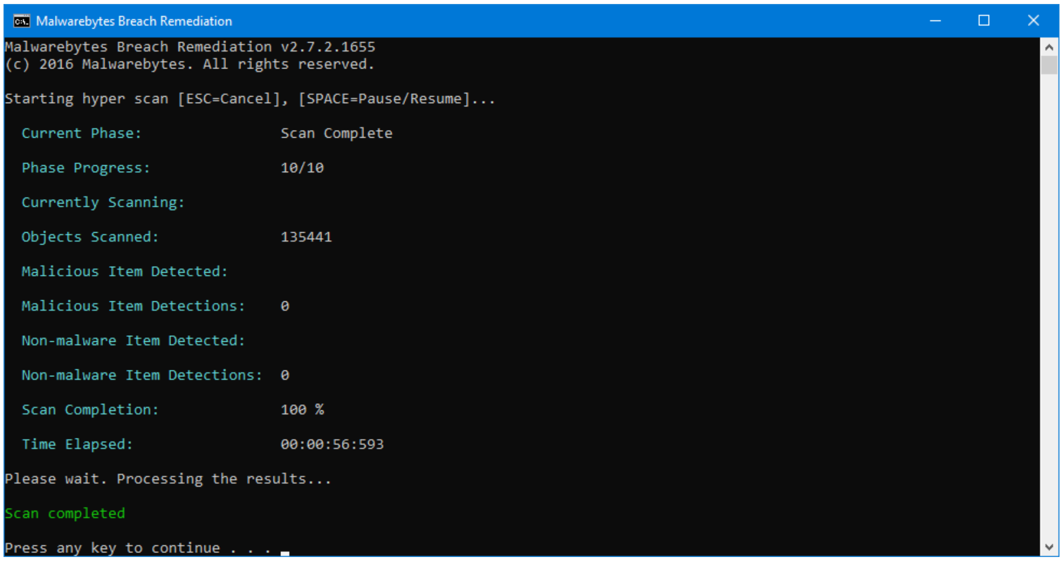
Malwarebytes Breach Remediation for Windows version 2.x and 3.x are included with *Malwarebytes Toolset* in the following locations and will need your *Malwarebytes Toolset* Product Key for licensing:

- Toolbox ▶ Remediate ▶ MBBR CLI Scan
- Toolbox ▶ Remediate ▶ MBBR Command Prompt
- Malwarebytes\MBBRv3\x64\mbbr.exe
- Malwarebytes\MBBRv3\x86\mbbr.exe
- Malwarebytes\MBBRv2\mbbr.exe

Malwarebytes Breach Remediation for Windows supports the following operating systems:

- **Version 3.**x: Windows 10, Windows 8.1, Windows 8, Windows 7 SP1, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, and Windows Server 2008 R2
- **Version 2.x:** Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows XP, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, and Windows Server 2003

For full details on how to use this utility, please read the Malwarebytes Breach Remediation for Windows User Guide. You can also run mbbr.exe from the Command Prompt with Administrator privileges with no arguments to a list of command line options, settings, and arguments.



```
Malwarebytes Breach Remediation v2.7.2.1655
(c) 2016 Malwarebytes. All rights reserved.

Starting hyper scan [ESC=Cancel], [SPACE=Pause/Resume]...

  Current Phase:                Scan Complete

  Phase Progress:               10/10

  Currently Scanning:

  Objects Scanned:              135441

  Malicious Item Detected:

  Malicious Item Detections:    0

  Non-malware Item Detected:

  Non-malware Item Detections:  0

  Scan Completion:              100 %

  Time Elapsed:                 00:00:56:593

Please wait. Processing the results...

Scan completed

Press any key to continue . . .
```

Malwarebytes Breach Remediation for Mac

Malwarebytes Breach Remediation for Mac is a portable GUI and Terminal version of *Malwarebytes for Mac* designed to facilitate malware remediation on macOS 10.9.5 or later. *Malwarebytes Breach Remediation for Mac* version 1.3.1 is available as a separate download and will need your *Malwarebytes Toolset* product key for licensing. You can obtain *Malwarebytes Breach Remediation for Mac* via the following methods*:*

- Download via the Check for Updates Tool
- Manual Download: https://downloads.malwarebytes.com/file/mbbr

For full details on how to use this utility, please read the *Malwarebytes Breach Remediation for Mac User Guides*. Links are included below.

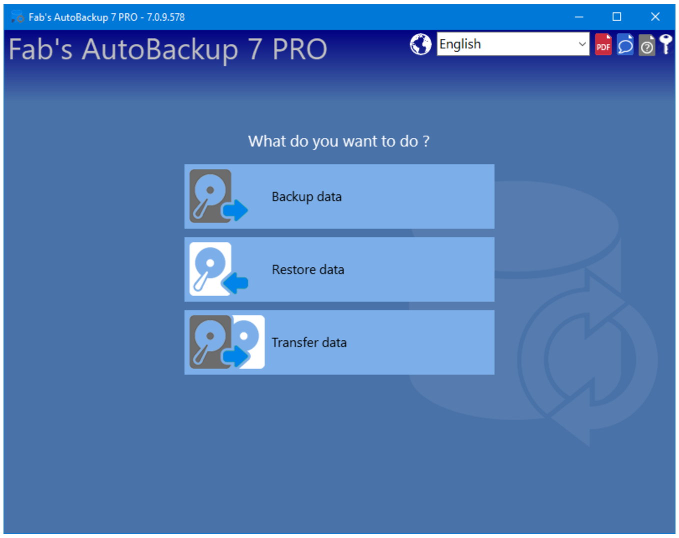
- GUI User Guide: https://www.malwarebytes.com/pdf/guides/MacRemediation-Client-AdminGuide.pdf
- CLI User Guide: https://www.malwarebytes.com/pdf/guides/MacRemediation-Client-CLI-AdminGuide.pdf

Fab's AutoBackup 7

To help expand the capabilities of the *Malwarebytes Toolset* and showcase one of our partners in the tech community, we have partnered with the wonderful Fabrice Parisot to bring access to *Fab's AutoBackup 7* to the Toolset (license not included). This utility is the industry leader for technicians that want to easily backup, transfer, and migrate user data and settings on Windows devices. You will find it under the Repair section of the Toolbox (and Malwarebytes\AutoBackup7Pro).

For more details on this product, check out the included user guide or visit the following website:https://www.fpnet.fr/

Please note that on first launch, *Fab's AutoBackup* will ask for your license info (for previous users), offer you an exclusive discounted license at 25% off (must be launched from the Toolset itself), or utilize a trial version of the product. Malwarebytes does not directly provide or sell these licenses, and it is up to you to obtain and provide one.



Frequently Asked Questions

Below are common questions users ask about using the *Malwarebytes Toolset*. If you have additional questions or need technical support, email our team the details at techbench@malwarebytes.com

► Getting Started - First Time Use

When you first use the *Malwarebytes Toolset*, you will need internet access to allow it to validate your license key and to update all components. To begin using the tool, perform the following:

1. Using the URL contained in your purchase confirmation email, download the *Malwarebytes Toolset*. Your license has been pre-injected into the product.
2. Extract the MBTS_X.X.X.XXXX.zip package file to the root of a USB flash drive or a dedicated directory within a USB Flash Drive.
    - **Please Note**: Ensure the path where the *Malwarebytes Toolset* has been extracted to does not contain any ASCII/UNICODE extended set characters.
3. Double click **MBTSLauncher.exe** from the extracted package.
4. Once the Toolset launches and validates your license, go to **Toolbox ► MyTools ► Check for Updates**
5. Download all available updates

For additional information on the features of the *Malwarebytes Toolset* and how to use them, please see the latest Malwarebytes Toolset User Guide and Malwarebytes Issue Scanner Technical Reference.

► How do I update the components of the *Malwarebytes Toolset*?

The *Malwarebytes Toolset* checks for a new release at launch. If one is available, an orange notification banner appears with an option to start an in-place update. For all other components, or to update manually, use the Check for Updates Tool by doing the following:

1. Launch the *Malwarebytes Toolset*
2. Click on the **Toolbox** component.
3. Go to **MyTools** and click **Check for Updates**
4. Select the components you want to update, then click **Download**
5. Follow any additional steps presented.

Any Toolbox item supported by the Updater can also be updated upon launch. If there is a new version, you have the option to download and use that one OR continue to use the older version.

► How do I run a malware scan?

We include a portable version of *Malwarebytes*, the *Malwarebytes Portable Scanner*. To use it, perform the following:

1. Launch the *Malwarebytes Toolset*
2. Click on the **Scan** component.
3. Click **Scan for Malware**.
4. Follow any additional steps presented.

By default, a malware scan will always prompt if you want to kill non-essential processes, check for database updates, and perform a Threat scan. If you want to change this default behavior, click on the **Settings** icon (it looks like a gear) and select **Edit Default Scan**.

If you want to perform a one-time custom scan, click **Custom Scan** and select the scan options you want to use.

► Does the *Malwarebytes Toolset* and/or *Malwarebytes Breach Remediation* support offline usage?

Both products support offline usage. The Toolset must be validated (required on first use) and updated. If these conditions are met, you can use the Toolset offline for seven (7) days with version 1.3 and fifteen (15) days with version 1.4+. If you are only using the *Malwarebytes Breach Remediation* command line utility, it supports fifteen (15) days of offline usage.

▶ How do I update the malware database/definitions?

By default, we always check for updates before a malware scan begins. Because you may be in situations with no internet access, we highly recommend updating the database/definitions at least once per day on an internet-connected PC. You can accomplish that two ways:

1. Launch the *Malwarebytes Toolset*
2. Click on the **Scan** component.
3. Click the **Settings**/gear icon next to *Malwarebytes Breach Remediation* and select **Run Manual Update**
4. Follow any additional steps presented.

– or –

1. Launch the *Malwarebytes Toolset*
2. Click on the **Toolbox** component.
3. Go to **MyTools** and click **Check for Updates**
4. Select the **Malwarebytes Rules** component and then click **Download**
5. Follow any additional steps presented.

▶ How do I scan for malware or issues from Command Prompt/Command-Line?

The *Malwarebytes Portable Scanner* and *Malwarebytes Issue Scanner* can be launched from the command line by passing **`/scan:malware`** or **`/scan:issues`** respectively to MBTS.exe or MBTSLauncher.exe. Below are examples of this:

- Malwarebytes Portable Scanner
    - **`MBTSLauncher.exe /scan:malware`**
    - **`MBTS.exe /scan:malware`**
- Malwarebytes Issue Scanner
    - **`MBTSLauncher.exe /scan:issues`**
    - **`MBTS.exe /scan:issues`**

If you need additional automation or scripting capabilities for malware scans, *Malwarebytes Breach Remediation for Windows* command line utility is included with the *Malwarebytes Toolset*. You can find it in the directory structure here:

- **`Malwarebytes\MBBRv3\x64\mbbr.exe`**
- **`Malwarebytes\MBBRv3\x86\mbbr.exe`**
- **`Malwarebytes\MBBRv2\mbbr.exe`**

You can also manually download it from here:.

- Malwarebytes Breach Remediation for Windows (3.x) - https://downloads.malwarebytes.com/file/mbbr3
- Malwarebytes Breach Remediation for Windows (2.x) - https://downloads.malwarebytes.com/file/mbbr

Alternatively, we provide a quick launching version of *Breach Remediation* in the Toolbox under the Remediate section. This is provided for instances where the GUI version is failing.

▶ How do I use AdwCleaner?

Malwarebytes AdwCleaner is included as a standalone component designed to remove adware, toolbars, and more. You can run it by doing the following:

1. Launch the *Malwarebytes Toolset*
2. Click on the **Toolbox** component.
3. Go to **Remediate** and click on **AdwCleaner**
4. Follow any additional steps presented.

▶ How do I use Malwarebytes Anti-Bundleware?

Malwarebytes Anti-Bundleware is a standalone tool designed to remove unneeded bundled software and junkware. You can use it by doing the following:

1. Launch the *Malwarebytes Toolset*
2. Click on the **Toolbox** component.
3. Go to **Remediate** and click on **Anti-Bundleware Scanner Beta**
4. Follow any additional steps presented.

▶ How do I scan for local network devices?

The *Malwarebytes Toolset* includes a Network Devices scanner to perform a detailed local network device inventory scan. To use it, perform the following:

1. Launch the *Malwarebytes Toolset*
2. Click on the **Inform** component.
3. Go to **Network** then click **Start Scan** under Network Discovery
4. Follow any additional steps presented.

▶ How do I check the SMART Attributes and Disk Errors on a disk drive?

The Disk Drive Issue Scanner of the *Malwarebytes Issue Scanner* performs this function. Please note that only failures or issues will be presented, but you can see full details by clicking on the Scan Report. To use the *Malwarebytes Issue Scanner*, perform the following:

1. Launch the *Malwarebytes Toolset*
2. Click on the **Scan** component.
3. Click on **Scan for Issues**
4. Follow any additional steps presented.

For additional information, please see the latest Malwarebytes Issue Scanner Technical Reference.

▶ How do I add tools?

The MyTools component of the *Malwarebytes Toolset* allows you to bring along additional tools, scripts, and batch files into the UI.

1. Launch the *Malwarebytes Toolset*
2. Click on the **Toolbox** component.
3. Go to **MyTools** and click **MyTools Editor**
4. Click the **+** icon to add a tool
   - To import a directory of tools, click the **Batch import** button instead (looks like a download icon)
5. Complete the Create Tool form and click **Save**

▶ How do I launch MyTools or Toolbox tools from Command Prompt/Command Line?

Any tool from the Toolbox (including myTools) can be launched from the command line by passing `/toolbox:"Name of Tool"` to `MBTS.exe` or `MBTSLauncher.exe`. These tools will be launched as Administrator and pass on the special variables defined in the MyTools section of the User Guide. Below are examples of this:

- *Malwarebytes AdwCleaner*
  - `MBTSLauncher.exe /toolbox:"AdwCleaner"`
  - `MBTS.exe /toolbox:"AdwCleaner"`

- Network Reset
    - `MBTSLauncher.exe /toolbox:”Network Reset”`
    - `MBTS.exe /toolbox:”Network Reset”`
- Windows PowerShell
    - `MBTSLauncher.exe /toolbox:”Windows Powershell”`
    - `MBTS.exe /toolbox:”Windows Powershell”`

► How do I download the Malwarebytes Toolset?

You can download the latest build of the *Malwarebytes Toolset* using the URL in your confirmation email. If needed, use the syntax below to manually obtain the *Malwarebytes Toolset* with your product key pre-injected:

- Standard Download: https://toolset.malwarebytes.com/file/mbts/YOUR-PRODUCT-KEY
- Full Download: https://toolset.malwarebytes.com/file/mbts_full/YOUR-PRODUCT-KEY

Alternatively, there are generic URLs if the auto-injection system is down/not working correctly.

- Standard Download (No Key): https://toolset.malwarebytes.com/file/mbts
- Full Download (No Key): https://toolset.malwarebytes.com/file/mbts_full

► What is the difference between the Standard and MBTS Full download of *Malwarebytes Toolset*?

The Standard download is a smaller package with only the following core components:

- *Malwarebytes Toolset* (Inform, Network Devices Scanner, Portable Scanner, Issue Scanner, and Toolbox)

Additional standalone components can be downloaded as needed when they are executed via the Toolbox or downloaded using the MBTS Updater by going to **Toolbox ► MyTools ► Check for Updates**.

The Full download is a larger package with the following core and standalone components:

- *Malwarebytes Toolset* (Inform, Network Devices Scanner, Portable Scanner, Issue Scanner, and Toolbox)
- *Malwarebytes Breach Remediation* v3 command line utility
- *Malwarebytes Breach Remediation* v2 command line utility
- *Malwarebytes AdwCleaner*
- *Malwarebytes Anti-Bundleware*
- *Malwarebytes Anti-Rootkit*
- *Malwarebytes for Windows* (installer)
- *Malwarebytes Support Tool*
- *Fab’s AutoBackup 7*