



TOOLSET

**Malwarebytes Toolset
Issue Scanner Reference**

22 February 2019



Notices

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

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

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

Copyright © 2018 Malwarebytes. All rights reserved.

Third Party Project Usage

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

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

Sample Code in Documentation

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

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

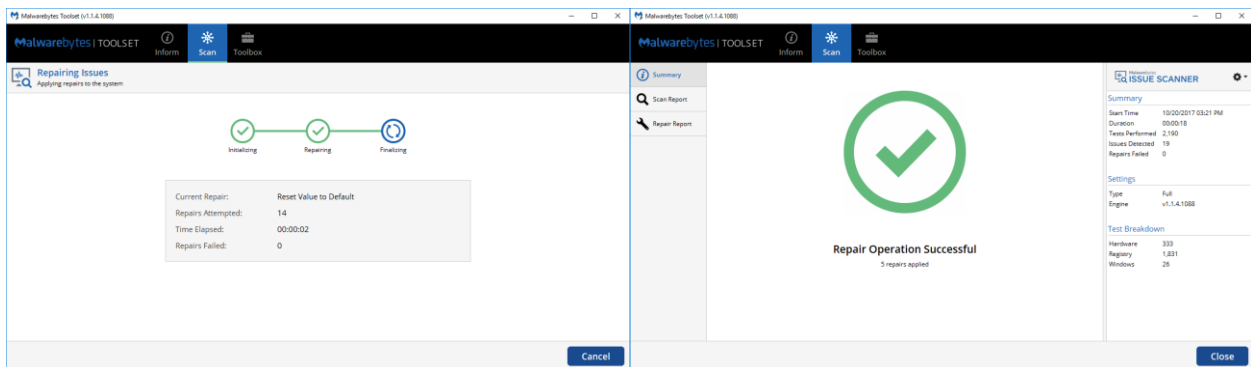
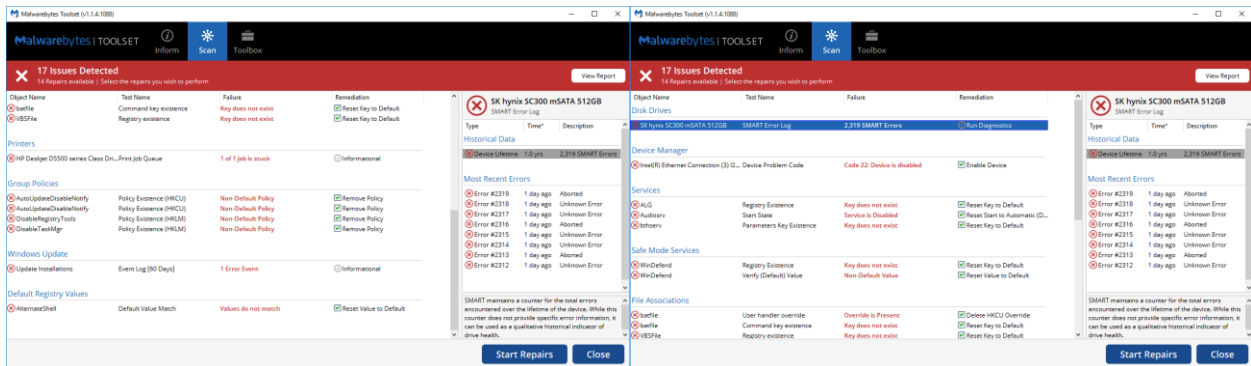
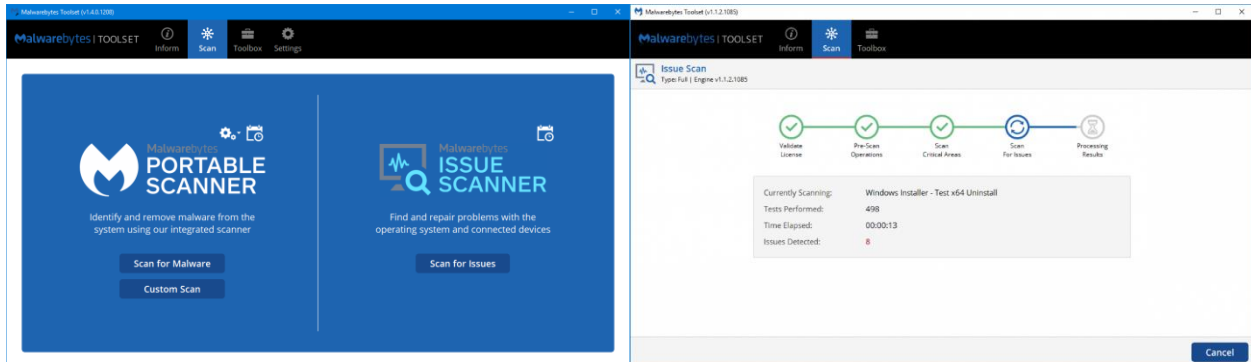
Table of Contents

Introduction	1
Supported Operating Systems.....	2
Technical Limitations	2
Hardware Issue Scanners	4
Disk Drive Issue Scanner.....	5
WHEA Issue Scanner	5
Device Manager Issue Scanner	5
Network Issue Scanner.....	6
Printer Issue Scanner	6
Registry Issue Scanners	7
Services Issue Scanner	8
Safe Mode Services Issue Scanner	8
File Associations Issue Scanner	8
Group Policies Issue Scanner.....	9
Default Registry Values Issue Scanner	9
Windows Issue Scanners	10
Windows Update Issue Scanner	11
Winsock Issue Scanner.....	11
WMI Issue Scanner.....	11
Windows Installer Issue Scanner.....	11
Reports and Scan Logs	11
Malwarebytes Issue Scanner Reports and Summary Log.....	11
Scan History.....	11
Other Log Files.....	13
Command Line Options	14

Introduction

The Malwarebytes Issue Scanner performs quick in-depth tests to identify and repair device issues. This can range from operating system issues to impending hardware failure. Depending on the issue scanner's capabilities, identified issues will have an associated automated repair OR provide detailed informational content so you can make an informed decision on next steps.

To run the Malwarebytes Issue Scanner, just open the latest version of the Malwarebytes Toolset and go to the Scan component. Then click Scan for Issues. A complete issue scan takes about one minute to complete.



Supported Operating Systems

The Malwarebytes Issue Scanner will run on any version of Windows but some will be skipped if we do not have OS profile data (e.g. Windows XP, Server, and Insider Preview builds) or if there is a technical limitation (e.g. .NET framework is missing but required, hardware doesn't support SMART, etc.).

In general, we support the following operating systems with all issue scanners (except when technical limitations occur):

- Windows Vista
- Windows 7
- Windows 8/8.1
- Windows 10

In general, the following operating systems will be limited to Hardware and a few Windows Issue Scanners (except when technical limitations occur):

- Windows XP
- Windows Server
- Windows Insider Preview

Technical Limitations

The following is a list of current technical limitations of some of our issue Scanners:

- The following issue scanners will be skipped if .NET 4.x is missing or corrupt:
 - Network Issue Scanner
 - Default Registry Values Issue Scanner
 - Windows Installer Issue Scanner
- SMART Attributes and SMART Status Check may be skipped on disk drives for one or more of the following reasons due to technical limitations:
 - The disk drive does not support SMART or a particular SMART Attribute
 - External storage device that does not provide SMART Passthrough
 - The disk drive uses NVMe and is running Windows 7/8.1
 - NVMe support is only on Windows 10 due to OS limitations
- The following issue scanners will be skipped if the operating system is Windows XP, Server, or Insider Preview:
 - Services Issue Scanner
 - Safe Mode Services Issue Scanner
 - File Associations Issue Scanner
 - Default Registry Values Issue Scanner
 - Winsock Issue Scanner

Hardware Issue Scanners

These Issue Scanners detect hardware related problems then provide detailed data to help one make an informed decision on next steps. Most will report back Informational content instead of offering an automated repair operation. Below are examples of a device with hardware issues. The first one shows the default results view while the second one shows an example of the SMART Error Log capabilities that appear in the Details Pane when that type of issue is found.

Malwarebytes Toolset (v1.1.2.1085)

8 Issues Detected
4 Repairs available | Select the repairs you wish to perform

Object Name	Test Name	Failure	Remediation
Disk Drives			
SK hynix SC300 mSATA 512GB	SMART Error Log	2,247 SMART Errors	Run Diagnostics
SanDisk Ultra Fit USB Device	Event Log [This Boot]	1 Error Event	Informational
Device Manager			
Microphone (Logitech Webcam C930e)	Device Problem Code	Code 22: Device is disabled	Enable Device
Integrated Webcam	Device Problem Code	Code 22: Device is disabled	Enable Device
Intel(R) Ethernet Connection (3) I218-LM	Device Problem Code	Code 22: Device is disabled	Enable Device
ECP Printer Port (LPT1)	Device Problem Code	Code 22: Device is disabled	Enable Device
Printers			
HP Deskjet D5500 series Class Driver	Print Job Queue	1 of 1 job is stuck	Informational
Network			
BITS Download Test	Download Test File	Couldn't complete BITS job	Informational

Malwarebytes ISSUE SCANNER

Summary

- Start Time: 10/06/2017 01:17 PM
- Duration: 00:00:18
- Tests Performed: 525
- Issues Detected: 8

Settings

- Type: Full
- Engine: v1.1.2.1085

Test Breakdown

- Hardware: 378
- Registry: 122
- Windows: 25

Unsupported Tests

- Unprofiled Operating System: 5

Start Repairs **Close**

Malwarebytes Toolset (v1.1.2.1085)

8 Issues Detected
4 Repairs available | Select the repairs you wish to perform

Object Name	Test Name	Failure	Remediation
Disk Drives			
SK hynix SC300 mSATA 512GB	SMART Error Log	2,247 SMART Errors	Run Diagnostics
SanDisk Ultra Fit USB Device	Event Log [This Boot]	1 Error Event	Informational
Device Manager			
Microphone (Logitech Webcam C9...)	Device Problem Code	Code 22: Device is disabled	Enable Device
Integrated Webcam	Device Problem Code	Code 22: Device is disabled	Enable Device
Intel(R) Ethernet Connection (3) I2...	Device Problem Code	Code 22: Device is disabled	Enable Device
ECP Printer Port (LPT1)	Device Problem Code	Code 22: Device is disabled	Enable Device
Printers			
HP Deskjet D5500 series Class Dri...	Print Job Queue	1 of 1 job is stuck	Informational
Network			
BITS Download Test	Download Test File	Couldn't complete BITS job	Informational

SK hynix SC300 mSATA 512GB
SMART Error Log

Type	Time*	Description
Historical Data		
Device Lifetime	1.0 yrs	2,247 SMART Errors
Most Recent Errors		
Error #2247	1 day ago	Aborted
Error #2246	1 day ago	Unknown Error
Error #2245	1 day ago	Unknown Error
Error #2244	1 day ago	Aborted
Error #2243	1 day ago	Unknown Error
Error #2242	1 day ago	Unknown Error
Error #2241	1 day ago	Aborted
Error #2240	1 day ago	Unknown Error

SMART maintains a counter for the total errors encountered over the lifetime of the device. While this counter does not provide specific error information, it can be used as a qualitative historical indicator of drive health.

Start Repairs **Close**

Disk Drive Issue Scanner

This will detect the following for currently attached disk drives and provide Informational guidance based results:

- SMART Status
- SMART Attributes/Errors
 - **5 - Reallocated Sector Count**
A total count of sectors marked as “reallocated” or remapped. This marking occurs when a read/write/verification error is encountered and the data is remapped to a special reserved/spare area of the disk. This is may indicate impending drive failure. Back up data and run additional drive diagnostics immediately. Hardware replacement may be required.
 - **187 - Reported Uncorrectable Errors**
A total count of errors that could not be corrected or recovered using hardware Error Correcting Code (ECC). This is may indicate impending drive failure. Back up data and run additional drive diagnostics immediately. Hardware replacement may be required.
 - **196 - Reallocation Event Count**
A total count of “reallocated” or remapped sector operations performed (successful and unsuccessful). If this value exceeds the Reallocated Sector Count (Error 5) that may indicate sector reallocation/remapping failures.
 - **197 - Current Pending Sector Count**
A total count of sectors waiting to be remapped due to a read/write/verification error. This is may indicate impending drive failure. Back up data and run additional drive diagnostics immediately. Hardware replacement may be required.
 - **198 - Uncorrectable Sector Count**
A total count of uncorrectable errors when reading/writing a sector.
 - **SMART Error Log (Historical Data - Device Lifetime)**
A count of all SMART Errors stored in the SMART Error Log and the length of time these errors occurred over. The time is based on device power-on time, not calendar time due to the technical limitations of SMART. While this does not provide specific error information, it can be used as a qualitative historical indicator of drive health.
 - **SMART Error Log (Most Recent Errors)**
A detailed list of the most recent SMART Errors stored in the SMART Error Log and the time they occurred. The time is based on device power-on time, not calendar time due to the technical limitations of SMART. Selecting one of these errors in the Details pane will display the full error details that are stored in the SMART Error Log. Due to technical limitations of SMART, only a limited number of detailed errors are stored in the SMART Error Log.
- Volume Dirty Bit
- Disk Free Space
- NTFS and Disk errors in Event Log (This Boot - External and Last 60 Days - Internal)
- Windows Failure Prediction Status

WHEA Issue Scanner

This will parse the Kernel-WHEA Event Log for hardware related failure that have occurred over the last 60 days and provide Informational based results.

Device Manager Issue Scanner

This will parse Device Manager Problem Codes and the Event Log for the Last 60 Days and report back any errors identified for all currently installed devices. If the Device Problem Code result is Device Disabled, you will be presented with the option to re-enable the device. All other results provided by this Issue Scanner is Informational only.

Network Issue Scanner

This will attempt to identify issues with network adapters and internet connectivity by doing the following and provide Informational based results:

- Check Windows for the current Internet Connectivity Status
- Perform a Basic Connectivity Test
 - Resolve the Default Gateway via IPv4 and IPv6
 - PING the Default Gateway via IPv4 and IPv6
 - Resolve the Host DNS via IPv4 and IPv6
 - PING the Host DNS via IPv4 and IPv6
- Perform a HTTP Download Test
 - Create a temporary file
 - Download a test file
 - Verify file signature
 - Delete temporary file
- Perform a BITS Download Test
 - Create a temporary file
 - Download a test file
 - Verify file signature
 - Delete temporary file

Printer Issue Scanner

This will check for stuck or corrupted print jobs in the Print Job Queue for all installed Printers. If a stuck or corrupted job is detected, you will be presented with the option to clear the Print Queue.

Registry Issue Scanners

Registry Issue Scanners detect problems within the Windows Registry. Most will provide an automated repair, but Event Log related items will only provide informational based results. All issues identified and repaired by this Issue Scanner are OS version, edition, and build specific. Below are examples of a device with several registry and Windows OS issues.

Malwarebytes Toolset (v1.1.2.1085)

Malwarebytes | TOOLSET Inform Scan Toolbox

24 Issues Detected 17 Repairs available | Select the repairs you wish to perform [View Report](#)

Object Name	Test Name	Failure	Remediation
Device Manager			
Msft Virtual CD-ROM ATA Device	Device Problem Code	Code 19: Invalid registry data	Informational
Standard floppy disk controller	Device Problem Code	Code 22: Device is disabled	Enable Device
Communications Port (COM1)	Device Problem Code	Code 22: Device is disabled	Enable Device
Services			
ALG	Registry Existence	Key does not exist	Reset Key to Default
Browser	ServiceDll Value	Non-Default Value	Reset Value to Default
Browser	Event Log [This Boot]	1 Error Event	Informational
bthserv	Parameters Key Existence	Key does not exist	Reset Key to Default
Safe Mode Services			
WinDefend	Registry Existence	Key does not exist	Reset Key to Default
WinDefend	Verify (Default) Value	Non-Default Value	Reset Value to Default
File Associations			
batfile	User handler override	Override is Present	Delete HKCU Override
batfile	Command key existence	Key does not exist	Reset Key to Default
VBSFile	Registry existence	Key does not exist	Reset Key to Default

Malwarebytes ISSUE SCANNER

Summary

Start Time 10/06/2017 11:27 AM
 Duration 00:00:13
 Tests Performed 1,874
 Issues Detected 24

Settings

Type Full
 Engine v1.1.2.1085

Test Breakdown

Hardware 136
 Registry 1,723
 Windows 15

Start Repairs **Close**

Malwarebytes Toolset (v1.1.2.1085)

Malwarebytes | TOOLSET Inform Scan Toolbox

24 Issues Detected 17 Repairs available | Select the repairs you wish to perform [View Report](#)

Object Name	Test Name	Failure	Remediation
Group Policies			
AutoUpdateDisableNotify	Policy Existence (HKLM)	Non-Default Policy	Remove Policy
AutoUpdateDisableNotify	Policy Existence (HKCU)	Non-Default Policy	Remove Policy
AutoUpdateDisableNotify	Policy Existence (HKCU)	Non-Default Policy	Remove Policy
DisableRegistryTools	Policy Existence (HKLM)	Non-Default Policy	Remove Policy
DisableTaskMgr	Policy Existence (HKLM)	Non-Default Policy	Remove Policy
NoDesktop	Policy Existence (HKLM)	Non-Default Policy	Remove Policy
Windows Update			
Last Update Search	Search Result [30 Days]	No searches have been attempted	Informational
Network			
Windows Status	Internet Status	Not connected to internet	Informational
Basic Connectivity	Resolve Default Gateway	Failed to resolve default gateway	Informational
HTTP Download Test	Download Test File	Unable to download windows updat...	Informational
BITS Download Test	Download Test File	Could not download using BITS	Informational
Default Registry Values			
AlternateShell	Default Value Match	Values do not match	Reset Value to Default

Malwarebytes ISSUE SCANNER

Summary

Start Time 10/06/2017 11:29 AM
 Duration 00:00:09
 Tests Performed 1,874
 Issues Detected 24

Settings

Type Full
 Engine v1.1.2.1085

Test Breakdown

Hardware 136
 Registry 1,723
 Windows 15

Start Repairs **Close**

Services Issue Scanner

We check the Services area of the registry (HKLM\CurrentControlSet\Services) for the following types of issues:

- **Default Services** (Services that are available by default in a base installation of Windows)
 - Registry Existence - Verify the object exists in the registry and offer to restore it if missing.
 - Start State - Verify this is set to the correct default setting and offer to restore it if incorrect
 - Service Type - verify this is set to the correct default setting and offer to restore it if incorrect
 - Parameters Key Existence - Verify the object exists in the registry and offer to restore it if missing. This will only run on Services that use this functionality.
 - ServiceDLL Value - Verify this is set to the correct default setting and offer to restore it if incorrect. This will only run on Services that use this functionality.
 - Event Log Errors This Boot - Report any errors that have occurred this boot by this Service
- **Installed Services** (Services that are not included by default with a base installation of Windows)
 - Event Log Errors This Boot - Report any errors that have occurred this boot by this Service

Safe Mode Services Issue Scanner

We verify that the entry exists and the values are correct for all default Services that are allowed in Safe Mode and Safe Mode with Networking. If a Service is missing or it's default value is set incorrectly, we offer to restore it.

File Associations Issue Scanner

We verify that File Associations for several default file types exist, are set to default, and do not have user overrides (commonly used by malware for hijacking).

Currently, we check the following File Extensions:

- .exe
- .bat
- .cmd
- .wsh
- .vbs

We do the following with each File Extension:

- User association override - Verify no override exists and if it does offer to remove it.
- Registry existence - Verify the object exists in the registry and offer to restore it if missing.
- Association Handler - Verify this is set to the correct default setting and offer to restore it if incorrect.

We also check the following File Handlers:

- exefile
- batfile
- cmdfile
- WSHFile
- VBSFile

We do the following with each File Handler:

- User handler override - Verify no override exists and if it does offer to remove it.
- Registry existence - Verify the object exists in the registry and offer to restore it if missing.
- Command key existence - Verify the object exists in the registry and offer to restore it if missing.
- Association Command - Verify this is set to the correct default setting and offer to restore it if incorrect.

Group Policies Issue Scanner

We check to see if any Group Policies are active that are commonly used by malware to prevent access to critical OS components and features. These are all Group Policies that are not enabled by default on a base installation of Windows. If we detect one is enabled, we offer to remove it. Please be mindful of these results on a PC in a controlled enterprise or business environment as some group policies may be in place legitimately.

Default Registry Values Issue Scanner

We check that several critical OS components are set to their correct default values. If they are missing or incorrect, we offer to restore them. We currently check the following:

- Winlogon - UserInit
- Winlogon - Shell (x86)
- Winlogon - Shell (x64)
- SafeBoot - AlternateShell
- Session Manager - BootExecute
- Session Manager - BootShell
- SubSystems - Kmode
- SubSystems - Windows

Windows Issue Scanners

Windows Issue Scanners detect problems with core components of Windows. Most will report back Informational content instead of offering an automated repair operation so you can make an informed decision on next steps or to draw focus to an area of the OS that is malfunctioning. Below are examples of a device with several registry and Windows OS issues.

Malwarebytes Toolset (v1.1.2.1085)

Malwarebytes | TOOLSET | Inform | **Scan** | Toolbox

24 Issues Detected | 17 Repairs available | Select the repairs you wish to perform | View Report

Object Name	Test Name	Failure	Remediation
Device Manager			
Msft Virtual CD-ROM ATA Device	Device Problem Code	Code 19: Invalid registry data	Informational
Standard floppy disk controller	Device Problem Code	Code 22: Device is disabled	Enable Device
Communications Port (COM1)	Device Problem Code	Code 22: Device is disabled	Enable Device
Services			
ALG	Registry Existence	Key does not exist	Reset Key to Default
Browser	ServiceDll Value	Non-Default Value	Reset Value to Default
Browser	Event Log [This Boot]	1 Error Event	Informational
bthserv	Parameters Key Existence	Key does not exist	Reset Key to Default
Safe Mode Services			
WinDefend	Registry Existence	Key does not exist	Reset Key to Default
WinDefend	Verify (Default) Value	Non-Default Value	Reset Value to Default
File Associations			
batfile	User handler override	Override is Present	Delete HKCU Override
batfile	Command key existence	Key does not exist	Reset Key to Default
VBSFile	Registry existence	Key does not exist	Reset Key to Default

Malwarebytes ISSUE SCANNER

Summary

- Start Time: 10/06/2017 11:27 AM
- Duration: 00:00:13
- Tests Performed: 1,874
- Issues Detected: 24

Settings

- Type: Full
- Engine: v1.1.2.1085

Test Breakdown

- Hardware: 136
- Registry: 1,723
- Windows: 15

Start Repairs | Close

Malwarebytes Toolset (v1.1.2.1085)

Malwarebytes | TOOLSET | Inform | **Scan** | Toolbox

24 Issues Detected | 17 Repairs available | Select the repairs you wish to perform | View Report

Object Name	Test Name	Failure	Remediation
Group Policies			
AutoUpdateDisableNotify	Policy Existence (HKLM)	Non-Default Policy	Remove Policy
AutoUpdateDisableNotify	Policy Existence (HKCU)	Non-Default Policy	Remove Policy
AutoUpdateDisableNotify	Policy Existence (HKCU)	Non-Default Policy	Remove Policy
DisableRegistryTools	Policy Existence (HKLM)	Non-Default Policy	Remove Policy
DisableTaskMgr	Policy Existence (HKLM)	Non-Default Policy	Remove Policy
NoDesktop	Policy Existence (HKLM)	Non-Default Policy	Remove Policy
Windows Update			
Last Update Search	Search Result [30 Days]	No searches have been attempted	Informational
Network			
Windows Status	Internet Status	Not connected to internet	Informational
Basic Connectivity	Resolve Default Gateway	Failed to resolve default gateway	Informational
HTTP Download Test	Download Test File	Unable to download windows updat...	Informational
BITS Download Test	Download Test File	Could not download using BITS	Informational
Default Registry Values			
AlternateShell	Default Value Match	Values do not match	Reset Value to Default

Malwarebytes ISSUE SCANNER

Summary

- Start Time: 10/06/2017 11:29 AM
- Duration: 00:00:09
- Tests Performed: 1,874
- Issues Detected: 24

Settings

- Type: Full
- Engine: v1.1.2.1085

Test Breakdown

- Hardware: 136
- Registry: 1,723
- Windows: 15

Start Repairs | Close

Windows Update Issue Scanner

We check that Windows Update has performed a search for updates in the last 30 days and that there are no outstanding Windows Update Installation Errors over the last 60 days.

Winsock Issue Scanner

We make a quick API call to verify the x86 and x64 Winsock Stack is functional.

WMI Issue Scanner

We perform a namespace connection and query to ensure WMI is functioning properly.

Windows Installer Issue Scanner

We perform a test install and uninstall of a special x86 and x64 MSI package that installs a test Service. This is done to check the integrity of the entire Windows Installer framework and process. We accomplish this by doing the following:

- x86 Install
 - Create Temporary File
 - Extract Installer
 - Check for Existing Install - Check Install Code, Product Code, Registry Key, App Location, and App Folder
 - Install x86 Installer
 - Verify Installation - Check Installer Log, Registry Key existence, and Service existence
- x86 Uninstall
 - Create Temporary File
 - Check for Existing Install - Check Install Code, Product Code, Registry Key, App Location, and App Folder
 - Uninstall x86 Installer
 - Verify Uninstallation - Check Uninstaller Log, Registry Key non-existence, and Service non-existence
 - Delete Temporary File
- x64 Install
 - Create Temporary File
 - Extract Installer
 - Check for Existing Install - Check Install Code, Product Code, Registry Key, App Location, and App Folder
 - Install x64 Installer
 - Verify Installation - Check Installer Log, Registry Key existence, and Service existence
- x64 Uninstall
 - Create Temporary File
 - Check for Existing Install - Check Install Code, Product Code, Registry Key, App Location, and App Folder
 - Uninstall x64 Installer
 - Verify Uninstallation - Check Uninstaller Log, Registry Key non-existence, and Service non-existence
 - Delete Temporary File

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.

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:

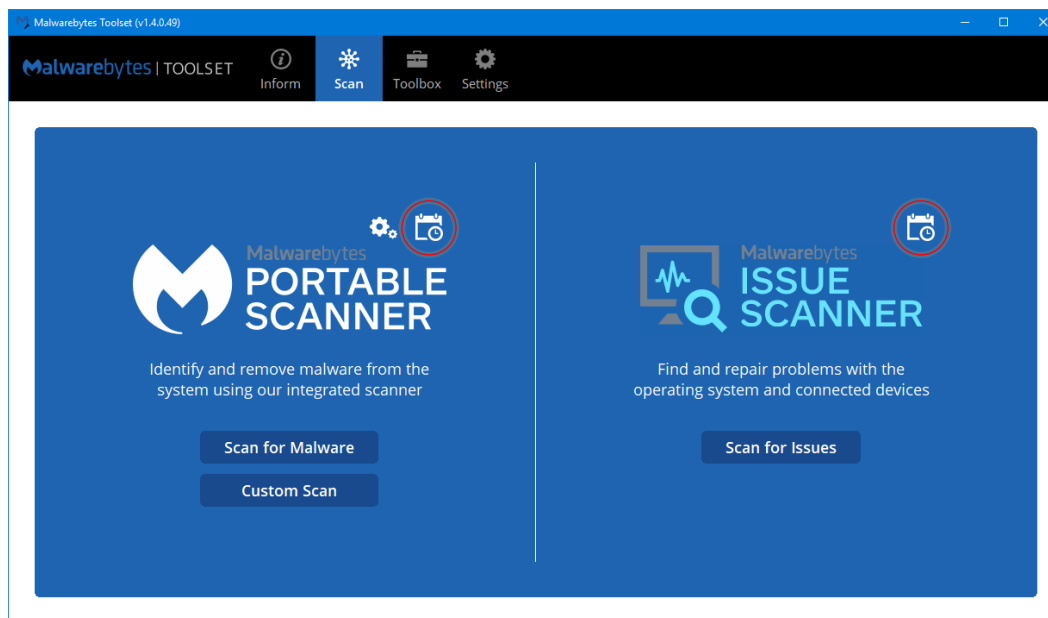
1. Go to **Scan** and click the **Scan History** icon (looks like a calendar) in the Malwarebytes Portable Scanner section
2. Select the scan report you want to load and click **View**
3. Click the gear icon near the top of the summary pane and select the desired operation:
 - a. Copy Summary to Clipboard – 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.

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.



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 03:24 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

View Delete Close

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

Malwarebytes TOOLSET | Inform | Scan | Toolbox | Settings

Malwarebytes PORTABLE SCANNER

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

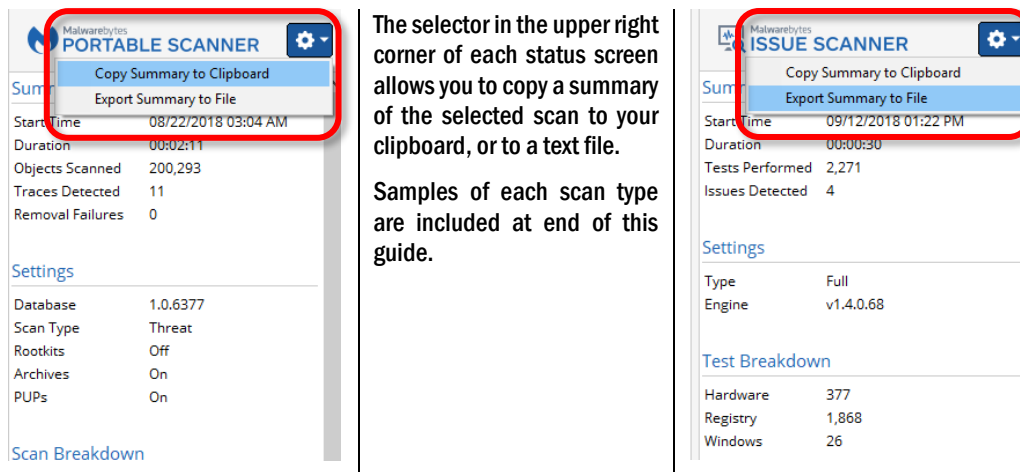
Scan Breakdown

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

Close

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.

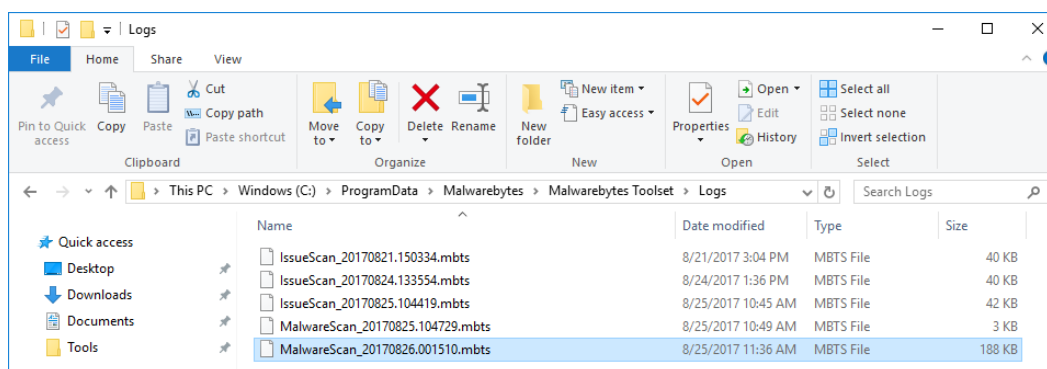
Each issue scan that is executed generates a log file. You may need this log file for troubleshooting purposes, or just for your records. Here's how to get that log. After running an Issue Scan, look for the Detail window associated with the scan, as shown here.



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.

By default, the Malwarebytes Toolset saves Scan History Log Files in `c:\ProgramData\Malwarebytes\Malwarebytes Toolset\Logs`. Since we store these files in a unique location on the PC itself, you can utilize this capability to transplant or share Scan History from on Windows PC to another. This is great for instances where you need someone else to see what the Toolset found, removes, and/or repaired. Keep mind that these files are compressed and encrypted so they can only be viewed in full by the Malwarebytes Toolset.



Other Log Files

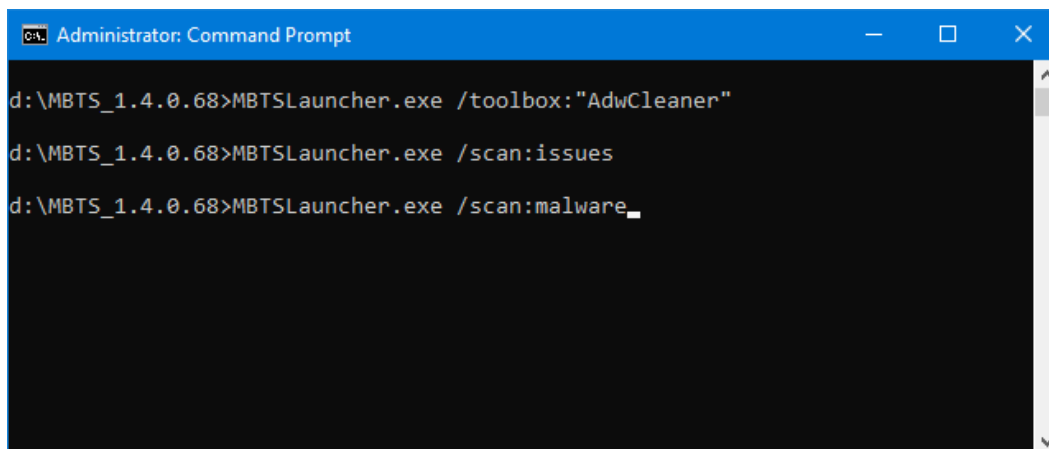
Additional log files are created for specific components that can help with customized reporting needs and troubleshooting. Below is a list of these with a brief description of their contents.

- `%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\MBRRv3\x64\Logs\MBRR-ERROUT.txt` -error and debug log files for Malwarebytes Breach Remediation CLI v3 64-Bit
- `\Malwarebytes\MBRRv3\x86\Logs\MBRR-ERROUT.txt` -error and debug log files for Malwarebytes Breach Remediation CLI v3 32-Bit
- `\Malwarebytes\MBRRv2\Logs\MBRR-ERROUT.txt` - the error and debug log file for Malwarebytes Breach Remediation CLI v2

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 the 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



```
Administrator: Command Prompt
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_
```