



Carbon Black Defense Sensor for Windows 2.0.4.9 Release Notes

April 28, 2017

Carbon Black, Inc.

1100 Winter Street, Waltham, MA 02451 USA

Tel: 617.393.7400 Fax: 617.393.7499

Email: support@carbonblack.com

Web: <http://www.carbonblack.com>

Copyright © 2011–2017 Carbon Black, Inc. All rights reserved. This product may be covered under one or more patents pending. Carbon Black Enterprise Response is a registered trademark of Carbon Black, Inc. in the United States and other countries. Any other trademarks and product names used herein may be the trademarks of their respective owners.

General Notes

Cb Defense Sensor version 2.0.4 is a GA (General Availability) release for the Windows operating system only. These notes are *cumulative*, and provide information on all 2.0 releases to date.

New Features

This section lists features introduced in the 2.0 version of Cb Defense Sensor. (For a more thorough description of the new features in this release, see the User's Guide.)

Enhanced Protection Engine

Cb Defense Sensor 2.0 contains many improvements in its engine that detects, blocks and reports malware. Specific improvements include:

- Improved offline protection through the introduction of a signature-based scanner
- Improved behavioral protection for attacks using PDFs, JARs, and macros

Note that the introduction of the signature-based scanner has introduced an additional log file (scanner\scanhost.log) and backend-dashboard options, including options that can be used to optimize performance.

Sensor Settings

- Allow Executable Uploads for Scans
- Show Sensor UI
- Allow User to Disable Protection
- Private Logging Level ⓘ
- Run background scan
- Scan files on network drives
- Scan execute on network drives
- Delay Execute for Cloud Scan
- Hash MD5

See the User's Guide for details about configuration of these new features.

New Cb Defense Sensor User Interface (UI)

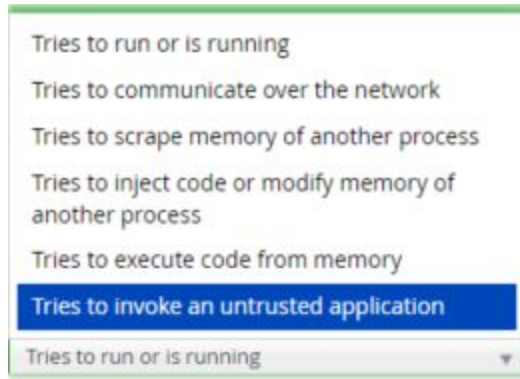
Cb Defense Sensor 2.0 contains a new client UI that can be enabled to notify end users when Cb Defense blocks the execution of suspicious software. The UI can also optionally be configured to allow the end user to enable and disable the Cb Defense Sensor's protection.

Enhanced Whitelist Capabilities

Cb Defense Sensor 2.0 contains enhanced whitelisting capabilities to make it easier for IT administrators to deploy enterprise software. Administrators can leverage a new "IT_TOOLS" whitelist option, and admins can specify that files signed with particular certificates are whitelisted.

Controlling Invocation of Untrusted Applications

Cb Defense Sensor 2.0 contains enhanced ability to control the invocation of untrusted applications.



Known Issues and Caveats

The following section lists known issues in this version of Cb Defense Sensor.

ID	Description
CIT-10882	Duplicate BLOCK or TERMINATE notifications will not be sent to the Sensor UI for a period of 30 minutes.
CIT-10780	An interoperability issue exists between the Cb Defense Sensor and McAfee 10.5 that can cause Microsoft Excel to exit immediately after launch. The problem relates to IPS (Intrusion Prevention System) functionality automatically enabled in 10.5 McAfee. The workaround is to disable the new IPS rules in McAfee. Note: The pre-existing McAfee default exploit protection can remain enabled.
CIT-10931	An interoperability issue between the Cb Defense Sensor and the Assima Training Suites application can cause Internet Explorer to crash. The workaround is to update Assima Training Suites to the latest version - this eliminates the Internet Explorer crash.

n/a	<p>Support for Windows XP, Windows Server 2003, and Windows Vista has been dropped in Cb Defense Sensor 2.0. See the User's Guide for details.</p> <p>Note: Users who need support for these legacy operating systems can continue to use the 1.x Cb Defense Sensor. Contact your Carbon Black account manager for details.</p>
CIT-10032	The "DELAY_SIG_DOWNLOAD=0" installer command-line option (which immediately updates AV signature definitions) cannot be used when upgrading the Cb Defense Sensor (the CLI option works for fresh installs only).
CIT-10273 CIT-10234	The Sensor User Interface's log file (RepUx.log) is in the <i>user's</i> temp directory (%TEMP%) rather than the <i>system</i> temp directory. Similarly, user-interface "mini-dump" files would be written to this same %TEMP% directory.
CIT-10904	<p>The local AV signature-based scanner in the Cb Defense Sensor can consume up to approximately 220 MB of memory on each Windows endpoint machine during normal operation.</p> <p>Note: The 2017-04-25 AV Signature Update reduced AV signature memory usage from approximately 260 MB to 220 MB.</p>
CIT-11060	The Cb Defense Sensor may prevent Windows Defender from removing malware. This is because the Sensor is preventing any and all access to the malware file.

Issues Resolved in 2.0.4

ID	Description
n/a	Support for Windows 10 "Redstone 2" (also called "Version 1703" and "Creators Update") was introduced with the 2.0.4 Cb Defense Sensor.
CIT-10906 CIT-10960 CIT-10961 CIT-10941 CIT-10978 CIT-10944 CIT-10989	Failed to install AV signature updates
CIT-10890	Whitelisted certs ignored when processing updated (NOT_LISTED) programs

CIT-10928	Sensor UI icon should reflect when Sensor in bypass mode
CIT-10972	Event log reports "CbDefense BACKGROUND_SCAN: COMPLETE" several times per day
CIT-10973 CIT-10986 CIT-10987	Endpoints rebooting without warning after "Update Sensors" push
CIT-10962	Certificate rules are not processing empty issuers correctly
CIT-10969	50-second delay processing default certificate policy
CIT-10827	Users not being switched to "Unassigned" after logging off of VDI
CIT-10951	Sensor log file reports that an application was blocked, but no events appear in dashboard web interface
CIT-10965	Improved ability to read signatures of files shared from remote devices
CIT-11009	Rundll32 script not detected
CIT-10887	High CPU utilization of Sensor process
CIT-11001 CIT-11002	Improve efficiency of processing shadow copy operations
CIT-10964 CIT-10971 CIT-10963 CIT-10251	Self-protection improvements
CIT-10981 CIT-10932 CIT-11020 CIT-11015 CIT-11014 CIT-11008 CIT-11007	General security efficacy improvements
CIT-10340	Support for "Tries to invoke a command interpreter" policy option (target availability in Cb Defense management console: late-May 2017)
CIT-10943 CIT-10946 CIT-10995	General stability and performance improvements
CIT-11012 CIT-11006	Improved diagnostics and logging

Issues Resolved in 2.0.3

ID	Description
CIT-10893 CIT-10845	Certificate name matching / Certificate whitelisting broken
CIT-8906	Improved handling/analysis of RTF (rich text file) content
CIT-10829	Improved handling/analysis of scripts (e.g., Powershell). Ensures that script host can be blocked while exempting certain scripts.
CIT-10345	Improved handling of script-based malware
CIT-9573	Improved handling of Java-based malware
CIT-10801 CIT-10816 CIT-10821 CIT-10822	General stability and performance improvements
CIT-10108	Sensor events not displayed on backend UI Alerts page.
CIT-10854	Remove explorer.exe false positive
CIT-10794	Issue retrieving AV signatures from local repositories using HTTPS
CIT-10818	Install Sensor even if user's temp directory not present
CIT-10585	Do not allow Sensor installation on Windows XP, Vista, and Server 2003
CIT-10885	Log file missing from diagnostics bundle
CIT-10903	Log file contains incorrect information on malware scan results

Issues Resolved in 2.0.2

ID	Description
CIT-10619	Improved expedited reputation request origination and handling when backend unreachable

DSEN-12	Honor signature-download randomization interval when signature scanning is disabled then re-enabled
DSEN-15	Increase default signature-download randomization interval to 4 hours. Support custom values from backend.
CIT-9507 CIT-10702 CIT-10703 CIT-10704	Reduce Cb Defense Sensor's memory and disk usage
CIT-8419	Incorrect IP Address information shown in Cb Defense Dashboard UI
CIT-10684	Improved detection of Javascript malware
CIT-9854	Improved throttling of events sent to backend
CIT-10553	Improved performance accessing local database
CIT-10714	Client UI now can display 'mailto' links

Issues Resolved in 2.0.1

The following section lists corrective content changes made.

ID	Description
CIT-10009	Internet Explorer 11 crash on Windows 10
CIT-9884	System error when processing IPv6 information
CIT-6545	Improved processing of app exclusions
CIT-6779	Improved detection of scripts invoked before Sensor start
CIT-10203 CIT-10204	Improved reputation processing and logging in a variety of corner-case situations, including when file certificate verification fails.
CIT-10119	Avoid instance of a false-positive script termination