Carbon Black.

Cb Response Windows Sensor

Release Notes

Version 6.1.4

March 2018

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

Introduction

This *Cb Response Windows Sensor Release Notes* document for version 6.1.4 provides information for users upgrading from previous versions as well as users new to the product. It consists of the following major sections:

- **Corrective Content and Improvements** – Describes issues resolved by this release as well as more general improvements in performance or behavior.
- **Known Issues and Limitations** – Describes known issues or anomalies in this version that you should be aware of.
- **Contacting Technical Support** – Describes ways to contact Carbon Black Technical Support, and details what information to have ready so that the technical support team can troubleshoot your problem.

This document is a supplement to the main Cb Response product documentation.

Purpose of this Release

The Cb Response v6.1.4 Windows Sensor release provides support for Windows 10 Ent LTSB (IoT), as well as performance improvements and bug fixes.

Note: Each Cb Response sensor release is cumulative and includes changes and fixes from all previous releases.

Documentation

The standard product documentation for Cb Response includes:

- *Cb Response User Guide* – Describes Cb Response feature functionality in detail, plus administrative functions.
- *Cb Response Server/Cluster Management Guide* – Explains how to install and manage Cb Response servers and clusters.
- *Cb Response Server Sizing Guide* – Provides details on infrastructure sizing for the Cb Response server.
- *Cb Response API* – Documentation for the Cb Response API is located at https://developer.carbonblack.com.

Additional documentation for specialized tasks and situations is available on the Carbon Black User eXchange at https://community.carbonblack.com/.

Sensor Support for Operating Systems and Server Releases

Cb Response sensors interoperate with multiple operating systems and Cb Response server releases.

- For the most up-to-date list of supported operating systems for Cb Response sensors (and all Carbon Black products), refer to this page in the Carbon Black User eXchange: https://community.carbonblack.com/docs/DOC-7991

- Cb Response sensors included with Cb Response server releases are compatible with all server releases going forward. However, they are incompatible with Cb Response server releases prior to the version they shipped with.

Technical Support

Cb Response server and sensor update releases are covered under the Customer Maintenance Agreement. Technical Support is available to assist with any issues that might develop during the upgrade process. Our Professional Services organization is also available to assist with the upgrade process to ensure a smooth and efficient upgrade installation.

Note: Before performing the upgrade, Carbon Black recommends reviewing content on the User eXchange for the latest information that supplements the information contained in this document.

Corrective Content and Improvements

Windows Sensor release 6.1.4.80222

This release includes the following corrective content changes and general improvements:

1. Fixed an issue where the sensor was not properly applying the site throttling limit set. [CB-14456]
2. Added support for Windows 10 Ent LTSB (IoT). [CB-15088]
3. Fixed an issue in which the sensor group noted in the Windows registry key was not being updated after a sensor was relocated. [CB-15713]
4. Fixed an issue where CbLR memory dumps could result in a bugcheck if the BIOS firmware misreported the valid physical address ranges. [CB-15801]
5. Improved performance of accessing files residing on mapped network drives. [CB-15846]
6. Fixed an issue with reporting Legal Trademarks in binary version info. [CB-15899]
7. Fixed an issue where sensor upgrade failures could result in the sensor being offline. [CB-16039]
8. Refactored critical code paths to improve performance on systems with heavy parallel workloads. [CB-16108, CB-16178]
9. Fixed an issue where binary collection disabled could lead to the services md5 mapping cache growing infinitely. [CB-16110]
10. Fixed an issue where waiting on system events could lead to a bugcheck. [CB-16650]
11. Updated the sensor.log file so that it reports process termination in decimal PIDs. [CB-16830]
12. Fixed an issue where suppressed processes were not being unsuppressed after a cross-process event was generated under medium suppression. [CB-16877]

13. Fixed an issue where certain return codes for object waits were being incorrectly evaluated. [CB-16982]
14. Added safeguard logic to prevent bugchecks in the event Cb drivers fail to fully initialize. [CB-17020]
15. Fixed an issue with leaked cbk7.sys object references upon driver shutdown. [CB-17039]
16. Removed the current working directory from the default DLL search order to help mitigate DLL hijacking scenarios. [CB-17150]
17. Fixed an issue where multiple concurrent calls to the Cb file system filter created a deadlock scenario. [CB-17290]
18. Changed volume attachment to prevent Cb filter volumes from attaching to raw or shadow copy volumes. [CB-17315]
19. Improved performance for calculating total file store size for all file store worker threads. [CB-17444]
20. Improved performance for registry callbacks under heavy workload scenarios. [CB-17445]
21. Created a default upload rate limit for Windows sensor until check-in message arrives with server value. [CB-17462]
22. Fixed an issue where the ‘sync’ command received from Cb server was not suspending previously set bandwidth throttle limits [CB-17490]
23. Fixed an issue where duplicate transactions were being recorded in the SensorComms.log. [CB-17491]
24. Fixed an issue where bandwidth throttling was not being applied outside main communication to server. [CB-17508]
25. Fixed a reference count issue with process contexts that could cause bugchecks to occur. [CB-17531]
26. Fixed an issue where the filestream contexts failed to lock themselves while updating cached name. [CB-17767]
27. Fixed an issue with sensor handling of unmounting system/filestore volumes. [CB-18071]
28. Fixed an issue where the service config communication could mishandle the file store disk space quota specified. [CB-18114]
29. Updated Curl to 7.58.0 and OpenSSL to 1.0.2n. [CB-18121]
30. Users now have the ability to disable DNS name resolution in data collection of network connection events when high CPU utilization is observed. See **Disabling DNS Name Resolution For NetConn Events** in the Known Issues and Limitations section for more details. [CB-17552]

Known Issues and Limitations

Disabling DNS Name Resolution For NetConn Events

Customers have observed that the Windows sensor can report high CPU utilization by the Carbon Black service ('cb.exe') on machines with a continuously large number of network connections (e.g., DHCP/DNS servers, Domain Controllers, etc.). To help alleviate the high CPU utilization without having to disable collection of network connection events, the Windows sensor can be configured to disable DNS name resolution in data collection for network connection events. This is done by editing the following Windows registry key as shown:

[HKEY_LOCAL_MACHINE\SOFTWARE\CarbonBlack\config]

"DisableNetConnNameResolution"=dword:00000001

Cb Entries Remaining in Add/Remove Programs

Customers uninstalling their Cb Response Windows sensor through uninst.exe will notice that Cb entries remain in the Add/Remove Programs window.

Cb Branding Is Different Between MSI and EXE Installers

Customers using the Add/Remove Programs window to manage their Cb Response installation should be aware that the Cb branding between the MSI and EXE installers is different.

Disproportionate Cb Logo on Install Wizard

Customers running the .exe installer may notice a disproportionate Carbon Black logo appearing on the Install Wizard

Install/Uninstall & Upgrade/Downgrade of Sensor on WinXP Requires Reboot

Customers running the Windows sensor on a Windows XP machine should note that a reboot of the machine will be required for all install/uninstall and upgrade/downgrade methods in order to successfully load and unload Cb drivers.

Cb Protection Upgrade Needed

Cb Protection includes a feature that tamper protects the Cb Response Sensor. If you are using both products and have not opted in to automatic updates of Cb Protection rules via the Carbon Black Collective Defense Cloud, you will need to manually update this tamper rule in order to successfully upgrade/downgrade Cb Response. For Cb Protection 8.0, you need the latest "Cb Response Tamper Protection" **Rapid Config**. For Cb Protection 7.x, you need the latest "Cb Response Tamper Protection" **Updater**. Please contact technical support to obtain the latest Rapid Config or Updater for Cb Protection.

Contacting Technical Support

Carbon Black Technical Support provides the following channels for resolving support questions:

Technical Support Contact Options
Web: User eXchange
E-mail: support@carbonblack.com
Phone: 877.248.9098
Fax: 617.393.7499

Reporting Problems

When contacting Carbon Black Technical Support, be sure to provide the following information:

Required Information	Description
Contact	Your name, company name, telephone number, and email address
Product version	Product name (Cb Response server and sensor version)
Hardware configuration	Hardware configuration of the Cb Response server (processor, memory, and RAM)
Document version	For documentation issues, specify the version of the manual you are using. The date and version of the document appear after the copyright section of each manual.
Problem	Action causing the problem, error message returned, and event log output (as appropriate)
Problem severity	Critical, serious, minor, or enhancement