Carbon Black.

Cb Response Cloud

Release Notes

Version 6.2.0

November 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

Introduction

The *Cb Response Cloud 6.2.0 Release Notes* document provides information for users upgrading from previous versions as well as users new to the product. It consists of the following major sections:

- New and Modified Features – Provides a quick reference to the new and modified features introduced with this version.
- Corrective Content – 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 Carbon Black Technical Support – Describes ways to contact Carbon Black Technical Support, and it 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 and Contents of this Release

The Cb Response 6.2.0 release contains new sensor versions, bug fixes, and stability and performance improvements. It packages the following component versions:

- Server – 6.2.0.171114.1606
- Windows Sensor – 6.1.2.71109
  Release Notes – https://community.carbonblack.com/docs/DOC-9772
- macOS Sensor – 6.1.2.71112
  Release Notes – https://community.carbonblack.com/docs/DOC-9773
- Linux Sensor – 5.2.13.71018
  Release Notes – https://community.carbonblack.com/docs/DOC-10153

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

Documentation

The standard user documentation for Cb Response product includes:

- *Cb Response User Guide* – Describes Cb Response feature functionality in detail, plus administrative functions.
- *Cb Response API* – Documentation for the Cb Response API is located at https://developer.carbonblack.com.

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

Supported Endpoint Operating Systems

For the most up-to-date list of supported operating systems for Cb Response sensors (and all Cb endpoint products), refer to the following page in the Carbon Black User eXchange:

https://community.carbonblack.com/docs/DOC-7991

Note: Non RHEL/CentOS distributions or modified RHEL/CentOS environments (those built on the RHEL platform) are not supported.

Technical Support

Cb Response server and sensor update releases are covered under the Customer Maintenance Agreement. Carbon Black recommends reviewing content on the User eXchange prior to performing the upgrade for the latest information that supplements the information contained in this document. Technical Support is available to assist with any issues that may develop during the upgrade process. Our Professional Services organization is available to assist with the upgrade process to ensure a smooth and efficient upgrade installation.

New and Modified Features

This release of Cb Response includes the following changes in functionality:

- VirusTotal feed has been removed from the user interface and documentation.
- The ***UserName*** **> Sharing Settings** page has a new option to enable diagnostic data collection on the server, either regularly or temporarily. Collecting this data in the background facilitate troubleshooting with Customer Support. The option is turned off by default.
- Cb Response now supports the IPv6 protocol.
    - Sensors can detect and process IPv6 IP addresses for the server to store and index. Communications between the server and sensors, however, use IPv4 protocol.
    - Cb Response can now recognize and process IPv6 keywords in the IOC (Indicators of Compromise) report section of custom feeds.
    - In searches and watchlist queries, you can specify IP addresses and address ranges in IPv6 Classless Inter-Domain Routing (CIDR) notation as well as in IPv4 format.
- Cloud customers can now access the following audit log records through syslog:
    - Cb Live Response session logs
    - Results of isolating a host
    - Results of removing a host isolation
    - Banning a file
    - Removing a file ban

Corrective Content

This release of Cb Response includes the following corrective content changes:

1. Fixed an issue in query-based Watchlist/Feed searcher so that it no longer returns false positives because missing fields in process metadata were replaced with “unknown” for some mandatory fields. (CB-15463)
2. Process search should now return results properly when using negated binary terms. (CB-13935)
3. The server will now properly handle Unicode strings when receiving sensor registration requests. (Cb-14484)
4. The UI will now allow the user page beyond the first 500 results in events. (CB-14668)
5. Banning hashes no longer results endless spinner. (CB-15337)
6. Process facet filters now update correctly when selecting another process the tree. (Cb-15351)
7. Binary_synchronizer now looks at all 256 possible values instead of just 16 values in the md5 hash field. (CB-15597)
8. Query builder now consistently displays the IPADDR parameter in an octet, instead of integer. (CB-13636)

Known Issues and Limitations

OS X Sensor Upgrade Limitation

Customers who have previously upgraded to OS X version 5.2.8.170419.1312 won’t be able to upgrade to OS X version 6.0.4.170328.1642 included in this package due to an installer issue that does not correctly allow for upgrade to a higher build version if the build timestamp is not newer. This does not affect any earlier OS X version built before March 28th, 2017.

OS X 10.12 Sierra Support with 5.2.0 Patch 3 and Later Sensors

If you have *already* upgraded to OS X 10.12 while running 5.2.0 Patch 2 or earlier versions of the sensor, the sensor will continue to operate, however certain events may not be reported as expected (for example, module loads) or some features might be unavailable (such as banning).

At this point, if the sensor is upgraded to 5.2.0 Patch 3 or later sensors, a reboot will be necessary to restore full functionality.

If 5.2.0 Patch 3 or a later sensor is installed *before* upgrading to OS X 10.12 or a fresh install of 5.2.0 Patch 3 or a later sensor on 10.12 Sierra **will not** require a reboot to begin functioning fully.

Using Boolean OR with Negated Query Terms

Cb Response server query language relies on the query syntax of the underlying database architecture that uses SOLR/Lucene. This query syntax has limitations when dealing with negated terms in queries that contains Boolean OR, for example, A OR -B.

In such cases, negated term is OR'ed with the result set of the terms that are not negated, instead of being applied first over the entire document set and then OR'ed with the result set of the other terms. This may return confusing search results, for example:

netconn_count:[20 TO *] OR -process_name:chrome.exe

This query is expected to return processes that have more than 20 network connections OR processes not named *chrome.exe*, regardless of their network connection count. However, the results set will be a set of processes that are not named *chrome.exe* in the set of processes that have more than 20 network connections.

In order to work around this shortcoming, the logical OR could be translated into a logical AND by using the equivalent negated version of the entire query, for example, A OR -B → -(-A AND B)

-(-netconn_count:[20 TO *] AND process_name:chrome.exe)

Alternatively, the negated term can be replaced with a term that includes logical AND to a term that would match all documents, for example:

netconn_count:[20 TO *] OR (process_id:* AND -process_name:chrome.exe)

A comprehensive fix to this limitation will be included in an upcoming release.

Tracking and Isolation of Network Connections that Existed Before the OS X Sensor Was Installed

In the OS X sensor version included in 5.1.1 Patch 2, we have made a design change to improve sensor interoperability with a number of other endpoint applications, for example, Symantec Endpoint Protection agent and LittleSnitch. This resulted in a modified behavior in tracking and isolation of network connections. In 5.1.1 Patch 2, network connections and sockets that are established *before* the sensor is installed will not be tracked for monitoring and isolation. If the machine is rebooted after installation, the sensor will continue to monitor and successfully isolate all network connections.

Other Issues

1. Cbssl command line throws a KeyError exception when run on the server, even though its execution correctly completes (CB-12622)
2. OS X and Linux sensors do not support excluding certain hashes from being banned via restrictions.conf. This feature is only supported for Windows platform.
3. Version 5.1.0 implementation of sensor purging has a known issue. If a sensor has been purged prior to its process data being purged, the Process Analyze page will return a 404 error for that sensors processes. All searching capabilities and process events are still present, searchable, and will be alerted.

To reduce the chances of this scenario if you choose to enable DeleteInactiveSensors, Carbon Black recommends setting your DeleteInactiveSensorsDays equal to or greater than your desired storage retention period. This issue has been addressed in 5.1.1 Patch 1.

4. Negated terms in queries with Boolean OR logic have some limitations (see section under upgrading the server). (CB-4068)
5. In order for sensor upgrades to work properly, McAfee EPO may need to be configured to exclude c:\windows\carbonblack\cb.exe from its "Prevent creation of new executable files in the Windows folder" option. (CB-7061)
6. The power state of a Linux sensor is not displayed correctly on the Host Details page. When a Linux sensor is powered off, the icon next to the Computer Name does not change to the correct state. (CB-6671)
7. Some outbound UDP network connections are not reported on Linux platforms. (CB-6630)
8. ICMP traffic is allowed when sensor is isolated on Linux and OS X platforms. (CB-6483/CB-6623)
9. Non-binary file write event collection cannot be disabled on Linux platforms. (CB-6686)
10. On OS X platforms, the UI setting to turn all “event collections” off is not honored. (CB-6389)
11. Binary execution of a file can still be banned if the file reuses the same inode on Linux and OS X platforms. (CB-6647/CB-6402)
12. If a sensor’s system clock is wrong and in the future, the start time for processes from that sensor are not displayed correctly in the Carbon Black console. (CB-6257)
13. On the Carbon Black server, when a sensor is moved out of a group with a user on a team that has only "Viewer" access to that particular group, results for that group are still searchable for the time period it was in that group, but the Process Details page links get 405 errors. If the sensor is put back into the group, the 405 errors for those processes go away. (CB-3704)
14. The Reshard tool can fail with “File Not Found” exception, in turn causing a corrupt index. If a re-shard is necessary, please contact support for a potential work around. (CB-3743)
15. The Linux sensor fails to properly cache observed events after the disk quota is reached and connection to the server is lost. (CB-6722)
16. The Linux sensor may fail to generate an MD5 and collect a binary image of file on a network share or user-space file system. (CB-6749)
17. CbEP enforcement fails after the Linux Sensor is uninstalled. A restart of CbEP is required to restore enforcement. (CB-7674)

Contacting Carbon Black Technical Support

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

Technical Support Contact Options
Web: www.carbonblack.com
Email: support@carbonblack.com
Phone: 877.248.9098 (877.BIT9.098)
Fax: 617.393.7499
Hours: 8:00 a.m. to 8:00 p.m. EST

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