

Carbon Black.



Cb Response Linux Sensor

Release Notes

Version 6.1.3
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>

Copyright © 2011–2018 Carbon Black, Inc. All rights reserved. This product may be covered under one or more patents pending. Carbon Black 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.

Introduction

The *Cb Response Linux Sensor v6.1.3 Release Notes* provide information for users upgrading from previous versions as well as users new to the product. It consists of the following sections:

- **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.
- **Contacting Technical Support** – Describes ways to contact Carbon Black Technical Support and what information to have ready.

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

Purpose of this Release

The Cb Response Linux Sensor v6.1.3 release includes support for RHEL 7.4, IPv6 event detection, a new explicit filter on binary file uploads, and additional bug fixes and performance improvements.

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 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](https://community.carbonblack.com/) 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 a comprehensive index of the operating systems that Cb Response sensors (and all Carbon Black endpoint products) support, refer to this page in the User eXchange:
<https://community.carbonblack.com/docs/DOC-7991>
- In general, version 6.x sensors work with 6.x but not 5.x versions of the Cb Response server.

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

Linux Sensor release 6.1.3.71227.1048

This release includes the following corrective content changes:

1. Added ability to detect IPv6 network events. (CB-9510)
2. Updated communications to the server to reduce CPU usage on the server.
3. Added support for RHEL 7.4, Centos 7.4, and Oracle RHCK 7.4. (CB-14201)
4. Fixed an issue where binary upload queue sizes were incorrect on the server. (CB-12904)
5. Fixed issue where local IP's were incorrect for UDP and TCP. (CB-13208)
6. Fixed issue where upload of binary or eventlog upload could cause CPU spike. (CB-13280)
7. Upgraded third-party libraries to most recent versions. (CB-14029, CB-16520)
8. Fixed issue which resulted in a small amount of dropped events each hour in high-volume cases. (CB-15910)
9. Fixed an issue where Fully Qualified Domain Name was not set properly. (CB-12733)
10. Fixed a few issues with the diagnostic script. (CB-14910, CB-15882)
11. Fixed an issue with reporting the correct path for a process in some cases. (CB-15789)
12. Fixed an issue where multiple daemons could be started at once on an endpoint. (CB-15850)
13. Fixed an issue where the daemon would not exit gracefully if not run as root. (CB-15851)
14. Added a safeguard to prevent the sensor from installing on unsupported kernel versions. (CB-15173)

Known Issues and Limitations

1. Sensor does not install on Oracle UEK 7.4 with 4.x kernel. (CB-17306)
2. Sensor Installer does not respect specified installation directory in the server. (CB-17033)
3. Warning message "eventlog quota exceeded" logged repeatedly when eventlog directory is full. (CB-16205)
4. The memory usage in the cbdaemon may increase due to the activity of some long-lived processes. A workaround is to restart the long-lived process or cbdaemon. (CB-16064)
5. Some of the tracking data in the kernel is using more memory than expected. This is most noticeable on systems with many long-lived processes. (CB-18105)
6. PID reuse on the system may cause new processes to not be suppressed when they should be. (CB-18239)
7. On RHEL/CentOS 6.x systems, upgrading a sensor from version 5.2.13 to version 6.1.3 causes a duplicate sensor to appear in the Server UI. See <https://community.carbonblack.com/docs/DOC-10841> for additional detail and a link to a workaround that hides the older sensor from the UI. (CB-1691)

Contacting Technical Support

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

Technical Support Contact Options
Web: User eXchange
Email: 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