Carbon Black Response
5.3.1 Release Notes

May 2017

Carbon Black, Inc.

1100 Winter Street, Waltham, MA 02451 USA

Tel: 617.393.7400 Fax: 617.393.7499

E-mail: support@carbonblack.com

Web: http://www.carbonblack.com

Introduction

The *Carbon Black (Cb) Response v5.3.1 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:

- **Preparing for server installation or upgrade**: This section describes preparations you should make before beginning the installation process for Cb Response server.
- **New and modified features**: This section provides a quick reference to the new and modified features introduced with this version.
- **Upgrading the Cb Response server**: This section provides information and instructions specific to server upgrades.
- **Corrective content:** This section describes issues resolved by this release as well as more general improvements in performance or behavior.
- **Known issues and limitations:** This section describes known issues or anomalies in this version that you should be aware of.
- **Contacting Carbon Black support:** This section 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 of this release

Cb Response v5.3.1 release contains *new sensor versions, bug fixes, and other stability and performance improvements.* It packages the following component versions:

- Server: 5.3.1.170523.0953
- Windows Sensor: 5.3.1.170426.1405
- OS X Sensor: 5.2.8.170419.1312
- Linux Sensor: 5.2.8.170427.1025

Documentation

The standard user documentation for Cb Response product includes:

- **Cb Response User Guide:** Describes Cb Response feature functionality in detail, plus administrative functions, including installing the Cb Response server and sensors.

- **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://github.com/carbonblack/cbapi.

Additional documentation for special tasks and situations is available on the Carbon Black User eXchange.

Preparing for server installation or upgrade

This section describes requirements to meet and key information needed before beginning the installation process for the Cb Response server. All users, whether upgrading or installing a new server should review this section before proceeding. Once you have reviewed this document, see the following for specific installation instructions:

- **To install a new Cb Response server**, see "Installing the Cb Response Server" section in the *Cb Response User Guide* for version 5.x
- **To upgrade a Cb Response server**, see Upgrading the Cb Response Server below in this document.

System requirements

Operating system support for the server and sensors is listed here for your convenience. The document *Cb Response - Server Sizing Guide* describes the full hardware and software platform requirements for the Cb Response server and provides the current requirements for systems running the sensor. Both are available on the Carbon Black User eXchange.

Both upgrade and new customers should be sure to meet all of the requirements specified here and in the Server Sizing Guide before proceeding.

Server / Console Operating Systems

- CentOS 6.4-6.9 (64-bit)
- Red Hat Enterprise Linux (RHEL) 6.4-6.9 (64-bit)

Installation and testing is done on default installs using the 'minimal' distribution and the distribution's official package repositories. Customized Linux installations must be individually evaluated.

Sensor Operating Systems (for endpoints and servers)

- **Windows**: XP SP3 - 10 / Server 2003 - 2012R2 and 2016 both x86 and x64

    - Windows embedded OSes are individually evaluated
- **Mac**: OS X 10.7 through 10.12.4, x64 on Intel
- **Linux:** RHEL & CentOS 6.4-6.9, 7.0-7.3 x64 – standard kernel versions (2.6.32-358.el6, 2.6.32-431.el6, 2.6.32-504.el6, 2.6.32-573.el6, 2.6.32-642.el6, and 3.10.0-123.el7, 3.10.0-229.el7, 3.10.0-327.el7,3.10.0-493.el7, 3.10.0-514.el7) and the standard minor/ maintenance releases. Non RHEL/CentOS distributions or Modified RHEL/CentOS environments (those built on the RHEL platform) are not supported.

YUM URL

Please use caution when pointing to the YUM repository. **Different versions of the product are available on different branches as shown below:**

- The current 6.1.0 (GA) version is available on Carbon Black YUM, pointed to by the following URL: baseurl=https://yum.distro.carbonblack.io/enterprise/stable/x86_64/
- The current 5.3.1 version is available on Carbon Black YUM, pointed to by the following URL: baseurl=https://yum.distro.carbonblack.io/enterprise/release/x86_64/

Note: Cb Response Server software packages are maintained at the Carbon Black YUM repository (yum.distro.carbonblack.io). Communication with this repository is over HTTPS and requires the presence of appropriate SSL keys and certificates. During the Cb Response server install or upgrade process, other core CentOS packages may be installed to meet various dependencies. The standard mode of operation for the YUM package manager in CentOS is to first retrieve a list of available mirror servers from http://mirror.centos.org:80 and then select one of those mirrors to download the actual dependency packages. If your Cb Response server is installed behind a firewall that blocks access to the outside, it is up to the local network and system administrators to ensure that the host machine is able to communicate with standard CentOS YUM repositories.

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.

Upgrading the Cb Response Server

Supported upgrade paths

Server upgrades to v5.3.1 are supported from the following previous versions:

- All 5.0 versions, including earlier patch releases
- All 5.1.x versions, including earlier patch releases
- All 5.2.x versions, including earlier patch releases

For more detailed instructions for installing or upgrading the server, please refer to the *Cb Response User Guide*. It is available on the Carbon Black User eXchange. For upgrading from earlier versions, please call or email Carbon Black Technical Support.

Configure sensor updates before upgrading server

If you are upgrading your server, you should determine if you would like to upgrade to the new *sensor* versions *before* you run the server upgrade program. Servers and sensors can be upgraded independently, and sensors can be upgraded by sensor groups, rather than all at once.

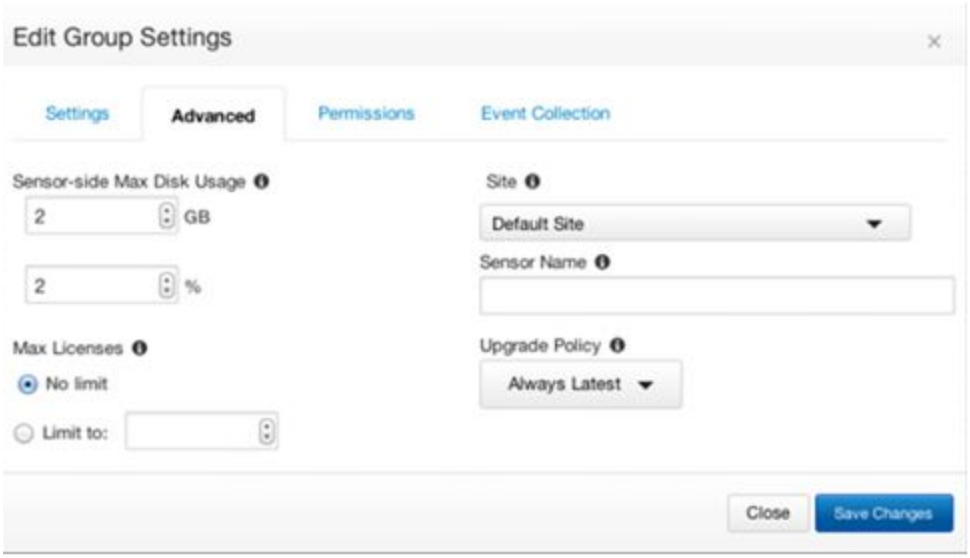
Decide if you would like the new sensor to be deployed immediately to existing sensor installations, or if you want to install only the server updates first. Carbon Black recommends a gradual upgrade of sensors to avoid any unacceptable impact on network and server performance.

Note: There is no expected degradation to sensor performance with Cb Response v5.3.1.

To configure deployment of new sensors via the Cb Response web UI follow the instructions below corresponding to the version you are upgrading from.

Versions 5.1.1 and below:

- Log in to the console, navigate to the Sensors page, and edit the group settings for each active Sensor Group:

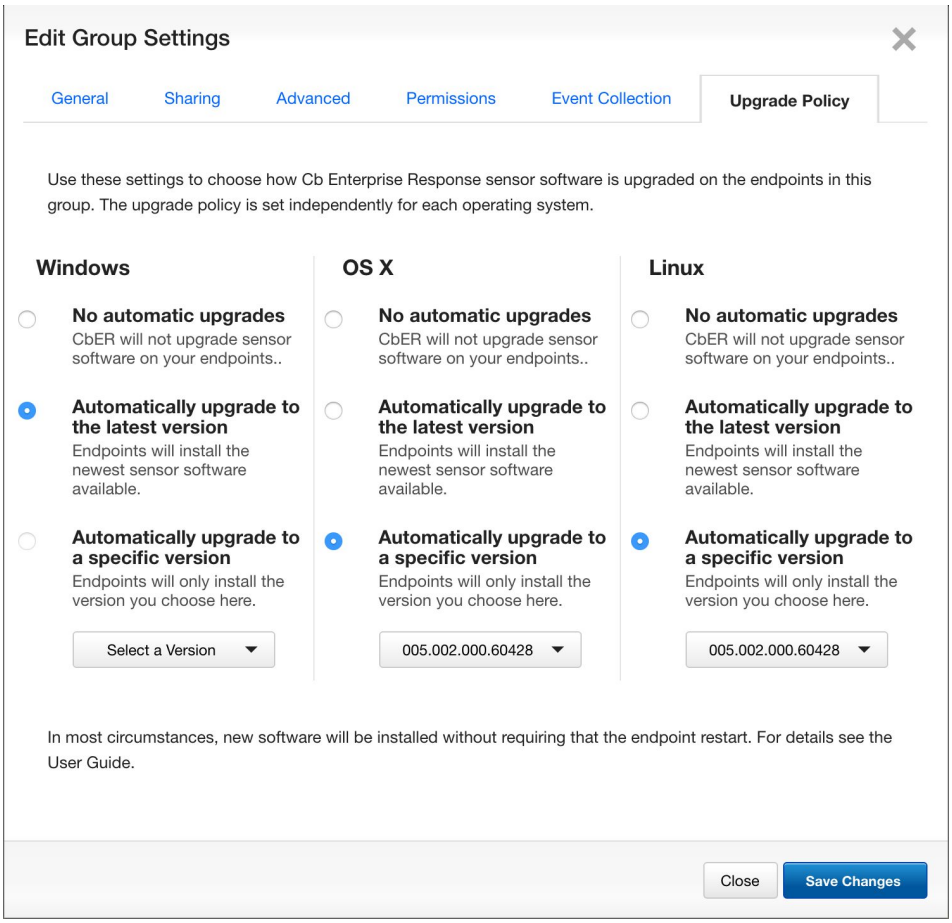


- Under the Advanced tab, find the Upgrade Policy setting. If this is set to **Always Latest**, the server will automatically upgrade sensors in this group to the latest sensor version.
  a. To keep the sensors at a specific version, select that version number from the dropdown prior to upgrade.
  b. To continue using whatever sensor versions are already installed, regardless of version, select **Manual**.

Note: Automatic upgrade settings for Sensor Groups apply to Windows sensors only. To change OS X and Linux sensor upgrade settings please see the “Installing Sensors” chapter of the *Cb Response User Guide*.

Versions 5.2.0 and above:

- Log in to the console, navigate to the Sensors page, and edit the group settings for each active Sensor Group:



- Under the Upgrade Policy tab, find the platform type you would like to configure. If this is set to **Automatically upgrade to the latest version**, the server will automatically upgrade sensors in this group to the latest sensor version.
  c. To keep the sensors at a specific version, select that version number from the dropdown prior to upgrade.
  d. To continue using whatever sensor versions are already installed, regardless of version, select **No automatic upgrades**.

Updating Cb Response server

If you are upgrading the server, please follow the steps in this section. These steps require SSH or console access to the server and minions with root privileges.

To upgrade a standalone server:

1. On the server, stop the Cb Response services: `service cb-enterprise stop`.
2. Update the Cb Response services: `yum update cb-enterprise`.
3. Restart the Cb Response services: `service cb-enterprise start`.

To upgrade a clustered server:

1. On the Master server, navigate to the cb install directory (defaults to /usr/share/cb) and stop the Cb Response services: `./cbcluster stop`.
2. Update the Cb Response services on each Master and Minion server node: `yum update cb-enterprise`.
3. On the Master server, restart Cb Response services: `./cbcluster start`.

Note: Improvements of Cb Response server will occasionally require using a utility called 'cbupgrade' (after `yum install/update cb-enterprise`) to migrate the database schema or alliance feed data. Upgrading from a previous stable version of Cb Response server to the current release does not require this step. However, running the utility is required when there are local changes to configuration files that have to be manually consolidated with the newer versions distributed by this release. The operator will be notified of this requirement when attempting to start the cb-enterprise services. In a clustered server configuration, this utility will need to be run on all nodes before restarting the cluster. *When running this utility in a clustered environment, be sure to answer 'NO' when asked to start server services; the administrator will need to use 'cbcluster' to start the clustered server.*

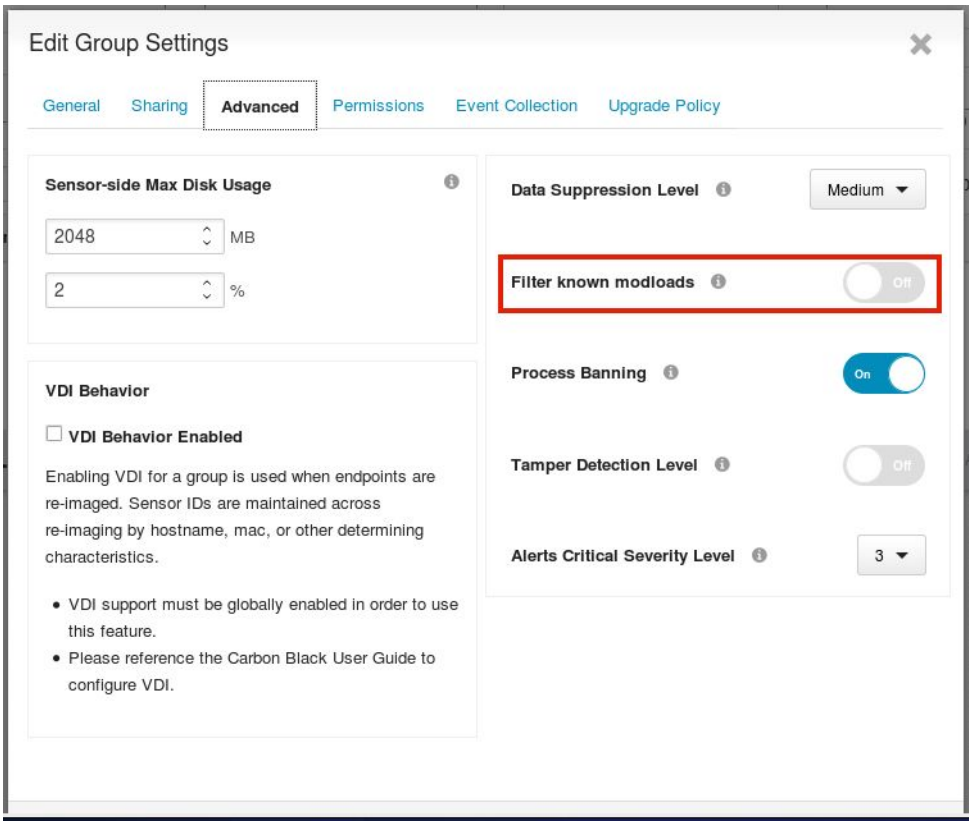
New and modified features

This section lists new and modified features in this version of Cb Response.

Cb Response 5.3.1 feature changes

Filter Known Binary Module Loads (extended supported on OS X)

Filtering of known Binary Module Loads (previously implemented in 5.2.0 as Windows platform only - Filter Known Windows DLLs) is now extended to OS X (requires 5.2.8+ OS X sensor) support and renamed as “Filter known modloads” under Sensor Group - Advanced settings tab to reflect the cross-platform support. This feature is disabled by default. The known modules on OS X are determined based on dyld_cache entries under /var/db/dyld.



Carbon Black recommends enabling this feature on OS X sensor groups, especially if endpoints are used for XCode software builds.

Cb Response 5.2 feature changes

The following sections provide a quick reference to the new and modified features introduced in version 5.2.0.

Eventless (Uninteresting) Process Suppression

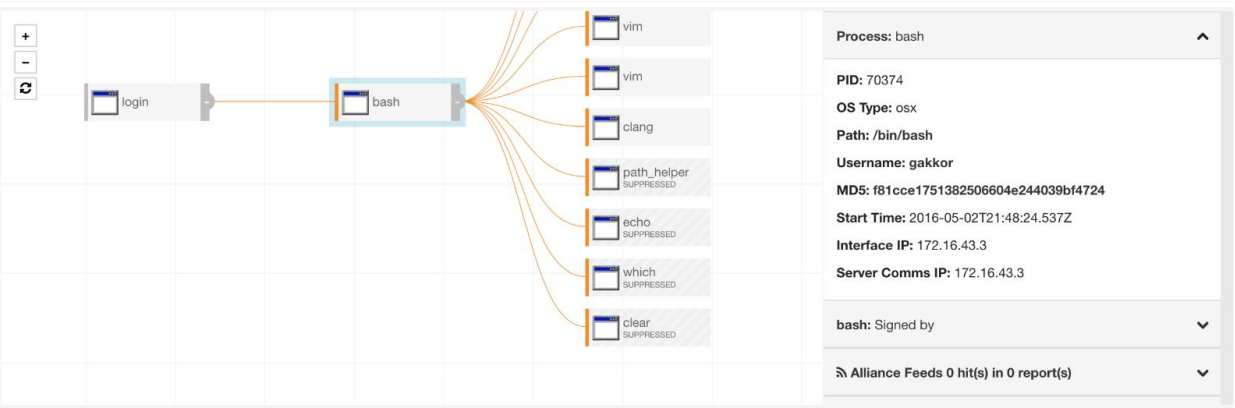
Starting with version 5.2, a process is classified as eventless (uninteresting) and therefore suppressed depending on the following definitions:

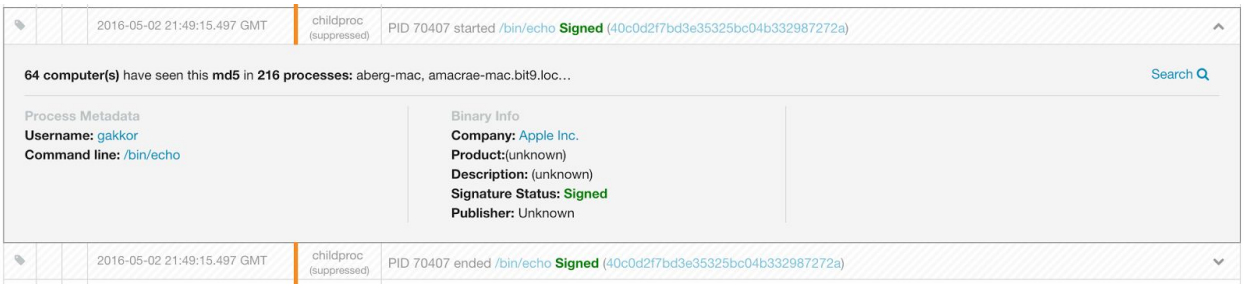
- **No suppression** - all processes are interesting, a process document is created for each process execution instance regardless of its activities and product works as before.
- **Medium suppression** - A process that has no network connections, file modifications, registry modifications, cross-process events, or child process events is classified as uninteresting. The only event in an uninteresting process would be module loads.
- **High suppression** - A process that has no network connections, file modifications, registry modifications or child process events is classified as uninteresting. The only events in an uninteresting process would be module loads and cross-process events.

What happens to the suppressed processes?

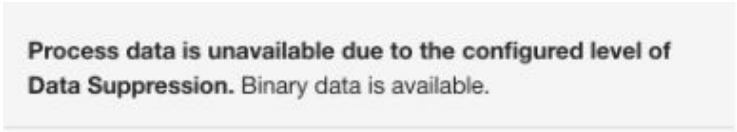
Suppressed processes are not stored/indexed by the server as stand-alone process documents. From the UI workflow perspective, this means that such processes will not have their own Process Analyze page; they can not be queried by process_name field. However, there is tracking of the execution of suppressed processes under the parent process. Version 5.2 expands the metadata details for the childproc event type under the parent to include, in addition to existing process and binary information metadata, command line and username information for suppressed processes. Such processes can still be searched by *childproc_name, childproc_md5, cmdline* and *username* field from the search pages.

The following figures show how Process Analyze page would look for a parent process that has suppressed child processes, in this example, **bash** has **echo**, **which**, **path_helper** and **clear** as suppressed child processes.





Note that there is no *Analyze* link within the event dropdown (since there is no process document), and if the process node were to be selected on the process tree, the metadata panel would warn you of the fact that this process is suppressed:



Eventless process suppression will have a pronounced impact on the number of process documents created by OS X and Linux sensors, e.g. many executions of *clear*, *cat, which*, and *ls* type commands on an OS X or Linux host will have reduced data processing impact on the deployment.

Frequently Asked Questions

- Suppression levels are configurable per sensor group basis from the UI.
- Suppression is supported on all endpoint platforms (Windows, Linux and OS X).
- Taking advantage of suppression features require upgrading endpoints and the server. to 5.2. Legacy sensors will report all events as before even if they connect to a 5.2 server with suppression enabled.

- On a new install or an upgrade, ALL existing sensor groups will have their suppression level set to MEDIUM by default. The server upgrade process will notify customers of this fact during upgrade. This can be later changed from the UI.

Improved POSIX process tracking

In previous versions of the Cb Response sensor, process tracking attempted to map each process fork and each process execution into unique process instances. This resulted in creation of a high number of process documents as forks that occur in POSIX environments don't always correlate with a new logical process. Additionally, the tracking of fork() system calls was not always accurate, which under some circumstances resulted in missed or incorrect process information.

In version 5.2, the OS X and Linux process tracking becomes more nuanced. POSIX process execution is now handled differently. First, any time a process performs a fork() system call, all activity for that process will continue to be associated with the parent. A new **"fork"** event type will be displayed on the Process Analyze page of the parent, indicating that the parent process performed a fork. The PID of the forked process and the timestamp of when the fork has occurred will be recorded. The first time a process (with a given PID) performs an exec() system call, a new process document will be created and the product will track the execution as a new logical process (current child process behavior). The create time for that new execution will be reported and will correlate to the timestamp when the process was created, that is when the fork occurred.

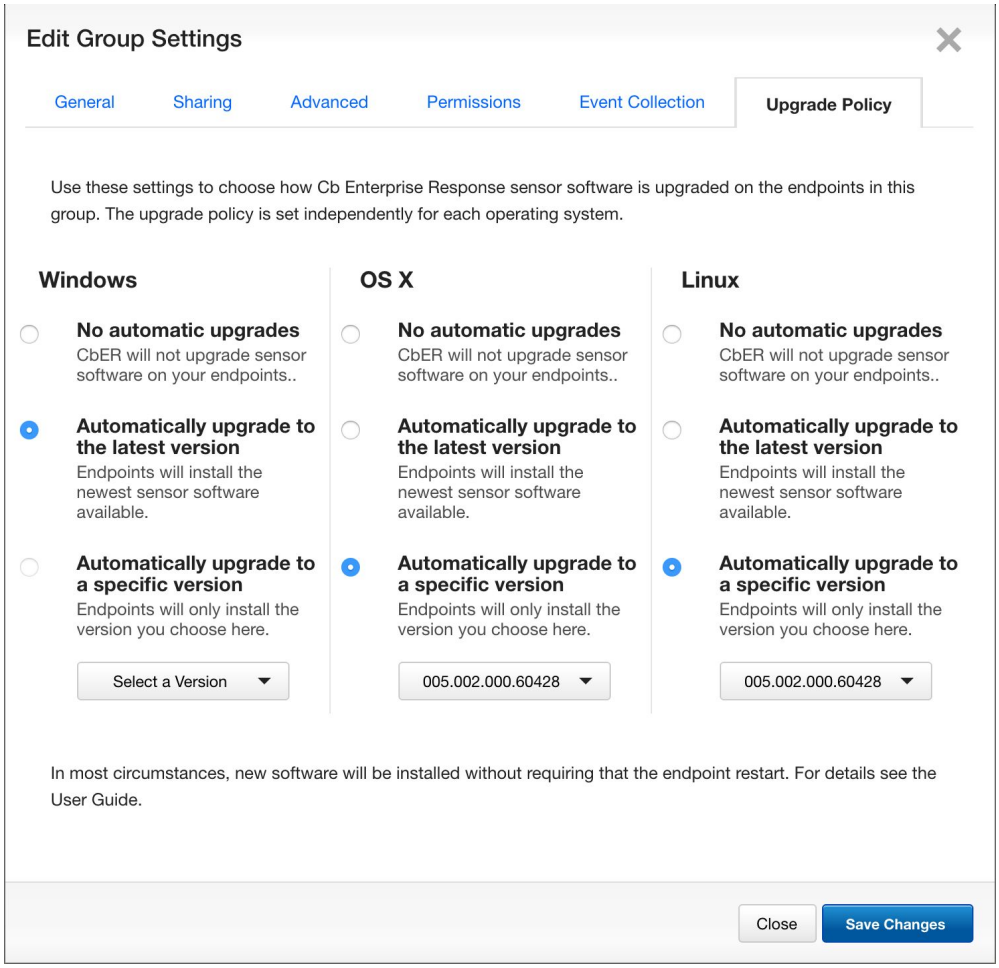
If at any point a process performs a second (or any subsequent) exec() system call, a new process document will **not** be created. This activity will be reported as a new **"exec"** event type within the process and the process meta-data will be updated to reflect the new image and command line associated with the exec() system call.

This new process tracking will reduce process document counts generated from OS X and Linux sensors considerably and give better visibility to different execution/instantiation paths. Fork and Exec type events apply only to OS X and Linux sensors. Windows sensors still report child process execution as before.

Support for the OS X and Linux sensor upgrades from UI

In this version, the OS X and Linux sensor upgrades become fully configurable and controllable via the UI. In previous versions of Cb Response, only the Windows sensor upgrade policy was configurable via the UI on a per-sensor-group basis. The OS X and Linux sensor upgrade policy applied globally to all sensor groups at once and had to be done by editing the cb.conf file.

With this version, the upgrade policy for all platforms can be configured from the UI and differ on a per sensor group basis. The new upgrade policy tab on the Edit Group Settings dialog is shown below:



Configuration options that existed for Windows sensor are now extended to OS X and Linux sensors. When upgrading from a previous version of Cb Response server, the following rules will apply:

- Configuration options previously set in cb.conf for upgrading the OS X and Linux sensors will be ignored.
- For all sensor groups, the OS X and Linux upgrade policies will be set to manual.
- Windows sensor upgrade policy will remain the same as what was previously set for each sensor group.

Other features and improvements

Suppression of known Windows DLLs

In this version, sensor group settings has a new option to enable suppression of known Windows DLLs. This is a Windows platform only feature. A known DLL is a Microsoft Windows term for basic DLLs that are loaded into RAM instead of being read from disk with every single process load. When this feature is enabled, trusted DLLs are simply not sent from sensor to the server on a per sensor group setting. More information on the definition of known DLLs can be found here:

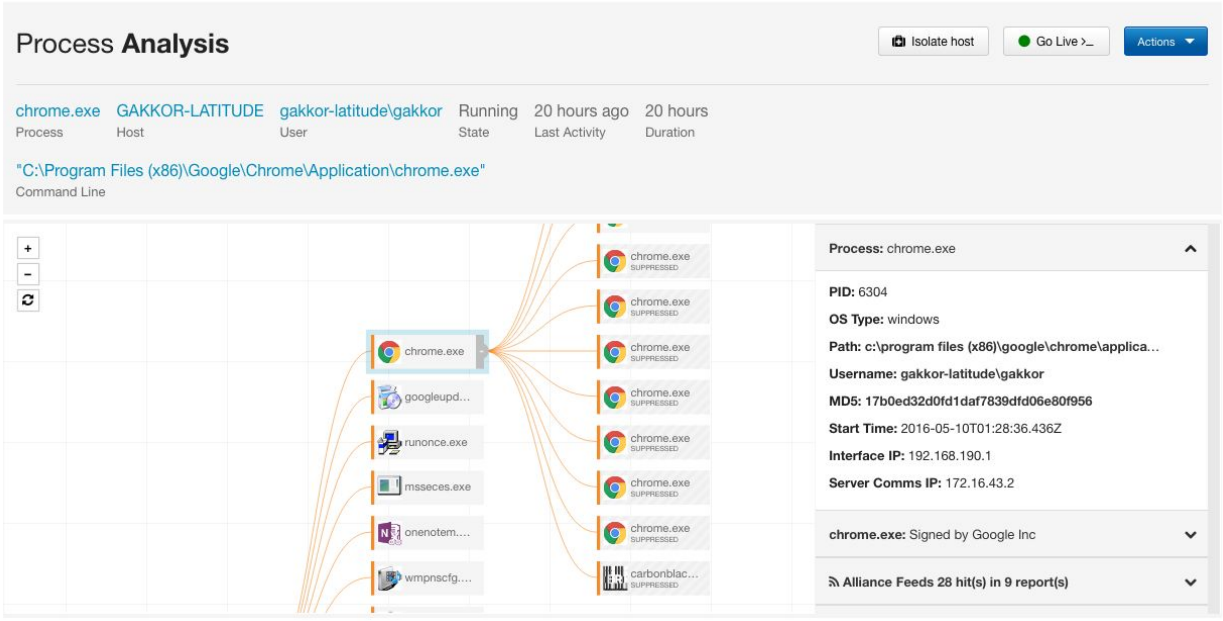
https://technet.microsoft.com/en-us/magazine/2007.09.windowsconfidential.aspx

Improved Triage Alerts page performance and workflow

In this version, Triage Alerts page is re-designed to load faster (with support for viewing more rows at a time) and provides a cleaner workflow for triaging alerts.

Redesigned Process Analyze page

In this version, Process Analyze page Process Information header and Process Tree view have been reworked to provide a cleaner look and richer content.



Cb Response 5.1.1 feature changes

The following sections provide a quick reference to the new and modified features introduced in version 5.1.1.

Endpoint isolation for Linux and OS X

The support for this feature, which was previously introduced in version 5.0.0 for Windows endpoints, has now been extended to include OS X and Linux endpoints. Requires 5.1.1 OS X and Linux sensor.

Responders can now instantly disrupt active intrusions by quarantining one or multiple endpoints from the network while still maintaining an active connection with the Carbon Black Response server. This enables IR (Incident Response) teams to perform more conclusive and surgical investigations, while limiting the damage from the attack.

Carbon Black live response for Linux and OS X

The support for this feature, which was previously introduced in version 5.0.0 for Windows endpoints, has now been extended to include OS X and Linux endpoints. Requires 5.1.1 OS X and Linux sensor.

Responders can now perform remote live investigations, intervene with ongoing attacks, and instantly remediate endpoint threats. This enables incident responders to “look at” and “touch” endpoints to take immediate action during an investigation, even while the endpoint remains isolated from the rest of the network—for example, by getting a real time file directory or killing a process running currently.

Custom endpoint threat banning for Linux and OS X

The support for this feature, which was previously introduced in version 5.1.0 for Windows endpoints, has now been extended to include OS X and Linux endpoints. Requires 5.1.1 OS X and Linux sensor.

With endpoint threat banning in Carbon Black Response, responders can now instantly stop, contain and disrupt advanced threats as well as block the future execution of similar attacks by banning binaries from being able to execute. This expands Carbon Black’s ability to drive additional corrective action on impacted endpoints as a part of incident response efforts.

Note: *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.*

Cb Response *Unified View*

Through a separate install package, the Carbon Black Unified View Server can be used to tie several clustered Cb Response deployments together with a unified user console. This capability allows for searching across multiple clusters with a unified result set.

Please refer to *Carbon Black Unified View Server User Guide* for more details on acquiring, deploying and maintaining Cb Unified View.

Splunk Integration

Carbon Black integration with Splunk is now available through the use of the Carbon Black Event Forwarder, which is located at the Carbon Black Github site. This connector takes feed and watchlist hits plus raw event data directly from Cb Response server, converts the data into JSON format, and allows the results to either be written out to a file or sent to a configurable destination. Combining the JSON output with the Carbon Black Technology Add-On provided by Splunk allows users to ingest Cb Response data into Splunk in a way that is compliant with Splunk's Common Information Model (CIM).

Please visit https://github.com/carbonblack/cb-event-forwarder for more details on the event forwarder and https://splunkbase.splunk.com/app/2790/ for information on the Carbon Black Technology Add-On.

Cb Response 5.1.0 feature changes

The following sections provide a quick reference to new and modified features introduced in 5.1.0.

Instant attack disruption & threat recovery with endpoint threat banning

With endpoint threat banning in Cb Response, responders can now instantly stop, contain and disrupt advanced threats. In addition, they can block the future execution of similar attacks by banning binaries from being able to execute. This expands Carbon Black's ability to drive additional corrective action on impacted endpoints as a part of incident response efforts.

Improved threat detection & kill chain analysis with Microsoft Enhanced Mitigation Experience Toolkit (EMET) integration

Cb Response 5.1.0 integrates with Microsoft's Enhanced Mitigation Experience Toolkit (EMET). This enables responders to correlate blocked exploitation attempts—from Microsoft EMET—with Carbon Black's collective intelligence to show key aspects of the attack both before and after the event. This empowers responders to optimize and improve their detection, investigation and patch management efforts by understanding the full kill chain of every exploitation attempt at the moment of compromise. SOC Personnel and incident responders can also have visibility into EMET configurations across an enterprise via this integration. This capability aids them in their investigations and allows them to properly determine the appropriate response.

Searchable threat intelligence reports

Providing new visibility and control into the threat intelligence feeds, Searchable Threat Reports allows visibility into the intelligence feeds. The visibility provided by the searchable reports includes insight into all indicators and queries contained within a feed. In addition, users can now suppress individual reports from triggering alerts to reduce false positive alerts for a feed.

Enriched threat intelligence with Damballa integration, domain reputation, geolocation & icon matching

Cb Response now leverages enhancements made to the Carbon Black Collective Defense Cloud's services: Attack Classification, Reputation and Threat Indicator Services.

- **Attack Classification:** The Collective Defense Cloud's Attack Classification Service provides comprehensive attack context and attribution by integrating with a robust list of industry-leading third-party sources to assist enterprises in identifying the type of malware and threat actor group behind an attack. The Collective Defense Cloud now delivers unmatched network-to-endpoint attack classification through its integration with

Damballa's leading threat intelligence on malicious destinations, advanced threat actor groups and command-and-control communications.

- **Reputation:** To optimize trust-based endpoint threat detection and response techniques, the Collective Defense Cloud now extends reputation to the network layer by delivering domain reputation—an excellent addition to its already unmatched reputation regarding known-good, known-bad and unproven software.
- **Threat Indicators:** To identify spear phishing campaigns that actively deceive end users by masking malicious activities under the appearance of trusted applications, the Collective Defense Cloud now provides icon matching to help detect social engineering attacks:
    - The Collective Defense Cloud also now provides geolocation look-ups of inbound and outbound network connections.
    - In previous releases, Cb Response tracked the destination port (the local port for inbound connections) and the remote IP address for network connections. In version 5.1.0, Cb Response tracks Local IP for both ends of the connection. (Note that search functionality is limited to destination port and remote IP addresses.)

Note: Access to these enhanced threat intelligence features requires data sharing with Carbon Black Collective Defense Cloud.

Enhanced threat inspection, analysis & correlation with Cyphort integration

Cb Response now integrates with Cyphort for inspection, analysis and correlation of suspicious binaries discovered at the endpoint. Now Carbon Black can submit unknown or suspicious binaries to Cyphort Core—a secure threat analysis engine, which leverages Cyphort's multi-method behavioral detection technology and threat intelligence—to deliver threat scores used in Cb Response to enhance detection, response and remediation efforts.

Resolving alerts as false positive and ignoring future events

In version 5.1.0, you have the option to resolve Alerts as false positives and go one step further by preventing the feed from alerting you to the same conditions in the future.

Corrective Content

The following section provides the corrective content changes made for each release.

Cb Response 5.3.1

Console and Server

1. Corrected a compatibility issue with Chrome 57+ browser version that caused Process Analyze page tree view to be rendered in the wrong location. (CB-13311)
2. Corrected an issue where Filemod facet in Process Analyze page showed Regmod events. (CB-12849)
3. Fixed an issue that caused sensor throttling algorithm to incorrectly compute the state and to stop ingest if an internal connection to Redis cache was momentarily lost. (CB-8472)
4. Corrected an issue where change directory command failed when using CBLR to view USB drives. (CB-11026)
5. Sharing settings are now correctly saved from the UI dialog when creating a new sensor group. (CB-13123)
6. Corrected an issue where some child processes are omitted from the Process Analyze page event rows when the PIDs are reused by the OS. (CB-13284)
7. Corrected an issue where pressing the enter key in Process Analyze page facets does not work. (CB-13356)

Windows Sensor (5.3.1.170426.1405)

1. Fixed multiple issues on sensor upgrades via GPO/MSI/EXE installers from previous version of sensors. (CB-12127, CB-13374, CB-13372, CB-13437, CB-13124)
2. Fixed two crashes due to NULL pointer reference in file operations context. (CB-13192, CB-13813)
3. Fixed an interoperability issue with 3rd party application Frostbite. (CB-13234)

OS X Sensor (5.2.8.170419.1312)

1. Corrected an issue where computing the MD5 hash of a file caused a crash. (CB-13742)
2. Corrected an issue that caused a kernel panic while waiting for the result of a MD5 hash during hash based banning execution. (CB-12980)
3. Corrected an issue that sometimes caused kernel panic during setup of dynamic library cache. (CB-12979)

Linux Sensor (5.2.8.170427.1025)

1. [NEW] Add CentOS/RHEL 6.9 support in 5.2-series sensor (CB-13430)
2. [NEW] Add CentOS/RHEL 7.3 support in 5.2-series sensor (CB-11511)
3. Major re-write of the Linux sensor to address high CPU, performance, stability, and accuracy (CB-12825, CB-6647, CB-12845, CB-13306, CB-11817, CB-11611, CB-11233, CB-11497, CB-12082, CB-9818)
4. Corrected an issue where MD5 hash was not calculated for all processes. (CB-12688)
5. Corrected an issue where receive UDP events were not correctly reported to the server. (CB-13815, CB-12258)
6. Fixed a possible crash when receiving UDP packets. (CB-13781)
7. Corrected an issue where sensor reported incorrect or incomplete process path information. (CB-8891)
8. Corrected several issues on install/upgrade of sensor daemon or kernel modules. (CB-12829, CB-13007, CB-132754, CB-13429, CB-11141, CB-9469, CB-10633, CB-11741, CB-11615, CB-8676)
9. Corrected an issue where proxied web network connections are not reported correctly. (CB-6669, CB-6714)
10. Corrected an issue where running process is not terminated when banned from server. (CB-12223, CB-12408)
11. Corrected an issue where banning a binary that has multiple running instances only terminates one of them. (CB-9731)

12. Corrected an issue where sensor health score reported as healthy even when the driver is not loaded. (CB-12119, CB-11964)
13. Corrected an issue where sensor stops sending event logs. (CB-11540)
14. Resolved an issue where some command line commands were reported as “-bash” instead of the full command details. (CB-6721)
15. Fixed multiple issues with CB Live Response. (CB-7512, CB-9024)
16. Added features to help Support with debugging. (CB-7576, CB-8963, CB-9277, CB-10994, CB-11487)
17. Multiple fixes to improve the performance and accuracy of network connection reporting. (CB-8830)
18. Corrected a potential interoperability issue with the CB Protection agent. (CB-11639)
19. Fixed an issue where CNAME’s were not always properly resolved. (CB-9638)
20. Added ability for sensor to report MD5 for non-binary files. (CB-9206)
21. Fixed an issue where the sensor could not communicate with the server in isolation mode if port was not specified in the URL. (CB-8238)

Cb Response 5.2.6

Console and Server

1. Fixed an issue where searching threat reports by IP address did not work. (CB-12164)
2. Fixed an issue where Sharing Settings tab values under Create Group dialog did not get saved. (CB-12569)
3. Fixed an issue where empty MD5 values are searched in unnecessarily while rendering Process Analysis page. (CB-12224)
4. Fixed an issue where PostgreSQL database failed to start after upgrade to 5.2. (CB-11897)
5. Fixed an issue where an Integer out-of-range error caused cascading entries in error logs. (CB-12447)
6. Hardened value validation for feed URLs when adding a new Threat Intelligence feed. (CB-11702)

OS X Sensor (5.2.5.170103.1147)

1. Fixes an issue where sensor installer required Xcode command lines tool. (CB-12347)

Linux Sensor (5.1.4.170131.1504)

1. Update third party OpenSSL package to 1.0.1b and Curl package to 7.50.3 (CB-12165)
2. Sensor now correctly reads disk quota values from sensorsettings.ini file (CB-12562, CB-12692)

Cb Response 5.2.5

Console and Server

1. Provide error context when users don't use full email addresses when entering SMTP configuration. (CB-11502)
2. Expose VirusTotal scores in email templates for process feed hits. (CB-11730)
3. Use correct non-default UI port in email templates. (CB-11525)
4. Fixed an issue that caused Triage Alerts page to fail rendering when an observed binary did not have digital signature information. (CB-11032)
5. Corrected an issue that caused attempts to ignore a threat report to fail when initiated from Threat Report Details page. (CB-10360)
6. Corrected an issue that caused entire query to be negated when the last group of terms in parenthesis is negated. (CB-11001)
7. Corrected an issue where selecting more than one item in Signature Status drop down menu in Add Criteria search fails with 500 error. (CB-11359)
8. Fixed an issue that caused logrotate.d postrotate script to fail for cb-rabbitmq component. (CB-11823)
9. Fixed an issue that caused logrotate.d postrotate script to fail for cb-rabbitmq in SELinux context. (CB-12042)

10. Corrected an issue where “sensors -a” command on a Cb Live Response session failed causing UI to hang indefinitely. (CB-11727)
11. Made RabbitMQ handshake timeout configurable to avoid partial services startup on environments that are slower. The new option, RabbitMQHandshakeTimeout is configurable via cb.conf. Default is 10000ms (results in effective timeout of 5000ms)
12. Corrected an issue where CSV export of events resulted in misaligned columns. (CB-12002)
13. Resolved an issue that resulted in process metadata with a command line that does not match the process name or path in Process Analyze page. (CB-11991)

Windows Sensor (5.2.1.161026.0747)

1. Fixed an issue where sensor provided MD5 hash of an empty string as an executable file hash to the server. (CB-11293)
2. Fixed an issue where disabling “network connections” event collection lowered the health score of the sensor. (CB-8851)
3. Fixed an issue where the sensor did not respect CarbonBlack\store\catalog file after a reboot causing increases IO load on each reboot. (CB-11509)
4. Fixed an issue where malformed values passed to sensor device driver (via malicious executables) can cause kernel panic due to device driver accessing invalid memory. (CB-8677)

OS X Sensor (5.2.4.161216.1642)

1. [NEW] Added support for OS X 10.12.1 version (CB-11663)
2. Fix an issue where installer set incorrect permissions to /Application/Carbonblack folder. (CB-11229)
3. Disabling “Non-binary Filewrite” event collection now works correctly. (CB-6491)
4. [NEW] Propagated event collection filters to kernel driver to improve sensor performance when collection for certain events are disabled. (CB-11510)
5. Added daemon-level awareness of incomplete/failed upgrades to avoid kernel panics. (CB-12187)

6. Fixed an issue with sensor using increased memory unders stress and causing endpoint to become unresponsive. (CB-9268)

Linux Sensor (5.1.2.161109.0849)

1. [NEW] Added support for RHEL/CentOS 7.3 version. (CB-11511)

Cb Response 5.2.0 Patch 3

Console and Server

1. Corrected an issue where Process Analyze page failed to render event rows for some processes that had events with milliseconds apart. (CB-10376)
2. Corrected an issue that prevented users from selected multiple values for sensor facets in the Sensors page. (CB-10387)
3. Corrected an issue where a spinner on the UI won't go away until page reload following a binary download. (CB-10486)
4. Restored user's ability to download all hosts to a CSV file. (CB-10768)
5. Resolved an issue with sorting of watchlist by name. (CB-10487)
6. Removed a duplicate "Unresolved" status facet from Triage Alerts page. (CB-10635)
7. Corrected the URL for "Community Watchlists" to point to correct User Exchange link. (CB-10718)
8. Restored rendering of Feed hits metadata in event rows detail. (CB-10640)
9. Corrected an issue with deleted users still getting alert notifications. (CB-10537)
10. Corrected an issue with alerts being generated for MD5 based IOCs that were marked as false positive. (CB-10810)
11. Fixed an issue with syslog messages using the CEF format template due to incorrect escaping of some characters. (CB-10274)
12. Added sensor interface and communication IP addresses to syslog notifications for Query-based Feed hits. (CB-10536)

13. Corrected an issue where database table for pending updates to Carbon Black Alliance server was purged too aggressively causing Threat Intelligence tags on some binaries to be missed. (CB-11212)

Windows Sensor (5.2.0.160922.1638)

1. Added support for Windows 10 Anniversary Edition. (CB-10444)

OS X Sensor (5.2.0.161003.1756)

1. Corrected an issue with binaries downloaded from UI was malformed. (CB-10494)
2. Corrected an issue with sensoruninst.sh script failing to completely uninstall the sensor. (CB-11029)
3. Corrected an issue with sensor occasionally creating unnamed processes. (CB-8907)
4. Corrected an issue where incorrect username is reported for some processes. (CB-10457)
5. Corrected an issue with sensor service crash on shutdown due to an extra reference count decrement. (CB-10326)
6. Resolved an issue which cause kernel panic on upgrading from previous versions of 5.1.1 and 5.2.0 under some load circumstances (CB-11224)

Cb Response 5.2.0 Patch 2

Console and Server

1. Corrected an issue where services failed to start if ModstorePath setting is changed from its default value in cb.conf (CB-8449)
2. [New Feature] Added ability to rate-limiting of feed hit events published on the enterprise bus by feed id and IOC value (default is OFF) (CB-8535)
3. Corrected an issue where a user with no team assignment could view all processes in the Search Processes page. (CB-8799)
4. Process Analyze page “Search Term” facet now works correctly. (CB-9169)

5. Process Analyze page “Filemod” facet now works correctly. (CB-9610)
6. Process Analyze page now correctly selects IP addresses from the IP facet dropdown. (CB-8988)
7. Selected facets now move up to the top of the list in Process Analyze page. (CB-9037)
8. “Ignore future events” option now correctly applied when marking alerts as “False Positive” (CB-9241)
9. Banned hashes list is now correctly sent to sensors when banning is enabled for a sensor group. (CB-8906)
10. Event purge cron job now does not fail if module store path is mounted on a different disk volume. (CB-8737)
11. Event purge now gracefully handles the case, where a binary set to be deleted is not available on disk. (CB-9401)
12. Feed hit notification e-mails no longer have truncated file/path names. (CB-10187)
13. When logging in as a non global admin, the login screen no longer continuously displays a spinning icon. (CB-10041)
14. Long command lines can now be copy/pasted easily from Process Analyze page header. (CB-9631)
15. FQDN with underscore is now allowed when entering server URL in sensor group settings dialog. (CB-4622)
16. The Sensor Details page now correctly shows upgrade policy settings. (CB-9232)
17. Corrected an issue where a single negated search term concatenated with Add Criteria terms fails to return results. (CB-9880)
18. [New Feature] Feed report ids are now included in the feed hit notification e-mails. (CB-9632)
19. Details of last banning attempt of a hash are now displayed correctly on the Banned Hashes page. (CB-9542)
20. An infinite spinner icon is no longer displayed on Process Analyze page if the process has no command line. (CB-10126)
21. Events can now can be added to Default investigations correctly. (CB-9487)

22. Corrected an issue where add new feed modal resulted in error on the Threat Intelligence page. (CB-9827, CB-9772)
23. Corrected an issue where event purge mechanism unnecessarily removed binary files stored under module store directory for purge metrics not tied to disk pressure. (CB-2789)
24. Users that are associated with existing investigations or banned hashes now can be deleted from the system without error (historical context/association continued to be maintained.) (CB-9317)
25. Improved Sensor Details page workflow - added pagination and ability to configure number of row displayed for a given set of search terms or facet selections (CB-9202, CB-9203, CB-9250, CB-9255, CB-9257)
26. Server now uniquely identifies alerts generated on ingress feed hits (e.g. from feed hit events feed.hit.ingress.process and feed.hit.ingress.binary) from alerts generated by the feed_searcher cron job nightly runs. While the former alerts only on new process executions or binary reports that match a given feed report, the latter also creates an alert when there is a change in the feed report content or score since the last time a process or binary was tagged. Alerts generated from feed_searcher cron job now have specific alert type that refers to “feedsearch” in name and are displayed in Triage Alerts page with yellow color instead of red for easy visual differentiation. (CB-9393)
27. New Triage Alerts page workflow now displays IOC value for IPv6, MD5, and domain under the source column in addition to feed report name. (CB-9627)
28. Corrected an issue where UTF-8 characters in process events caused exceptions in the SOLR datastore negatively impacting data ingest (CB-10424)
29. Corrected an issue where clicking on the hyperlink for IP address on a netconn event produced an error (CB-10403)
30. Corrected an issue where hyperlinks to Process Analyze page from process alerts were invalid (CB-10592)
31. Corrected an issue where Process Analyze page failed to render events because some event timestamps were missing in the API response (CB-10097)

Windows Sensor (5.2.0.160824.0930)

1. Improved sensor operation efficiency to reduce overhead during boot time (CB-8232, CB-9748)

2. Sensor no longer trigger AV alert during EICAR test signature in code (CB-9396)
3. [NEW] Added support for Windows 10 Anniversary Edition.

OS X Sensor (5.2.0.160721.1909)

1. Corrected an issue where sensor service was not stopping correctly causing problems during uninstall/shutdown. (CB-10127)
2. Sensor now correctly reports module load of an executable image. (CB-8491)
3. Sensor now correctly computes MD5 with lastWrite filemod events. (CB-9207)
4. Sensor now correctly synchronizes banning status with server on startup. (CB-9190)
5. Sensor now correctly reports lastWrite filemod events. (CB-9140)
6. Corrected an issue where invalid/truncated MD5 hashes were reported for binaries (CB-10095)

Cb Response 5.2.0 Patch 1

Console and Server

1. Corrected an issue where setting cb.conf option SensorLookupInactiveDays=X for limiting Sensor Details page view to sensors that have been active in the past X days fails with exceptions in coreservices debug logs. (CB-9593)
2. Corrected an issue where parsing of malformed filemod events causes exceptions in datastore, leading to poor data ingest performance. (CB-9514)
3. Corrected an issue where resolving multiple alerts as “false positive” failed with exceptions. (CB-9491)
4. Corrected an issue where Feed Reports in Threat Intelligence page failed to render if they contained IOCs that referred to binary documents. (CB-9422)
5. Corrected an issue where expanding child process terminate event rows in Process Analyze page UI showed incorrect information. (CB-9403)
6. Corrected an issue where process or binary path metadata for alerts created from query based feeds were truncated. (CB-9185)

7. Corrected a text box overrun in Ban Hashes" page. (CB-9173)
8. Improved service bus topology around watchlist/feed hit events to reduce traffic when those events are not of interest to anyone. (CB-8536)

Windows Sensor (5.2.0.160603.1453)

1. Corrected an issue where storefile disk quota (for storing binary files on sensor) may be exceeded. (CB-8447)
2. Corrected a rare bugcheck that occurred in the cbk7.sys sensor driver. (CB-9328)
3. Corrected a potential issue where sensor service caused divide-by-zero exception. (CB-6839)

OS X Sensor (5.2.0.160603.1436)

1. Fixed an issue where sensor install pkg file triggered an AV alert with EICAR test signature. (CB-9392)
2. Corrected an issue where sensor allowed banning of its own service. (CB-9397)
3. Corrected an issue where already running process failed to terminate if it ignored SIGTERM signal. (CB-9403)
4. Corrected an issue where suppressed child process reported within the parent process context did not have an unique process identifier. (CB-9316)
5. Corrected an issue where some child process terminate events were missed. (CB-9233)
6. Sensor now correctly reports CNAMEs in network connection events. (CB-9549)
7. Child process terminated events now correctly report the timestamp of end event, rather than the start event. (CB-9357)
8. Corrected an issue where remote commands executed via Cb Live Response left behind zombie processes. (CB-9193)
9. Corrected an issue where force umount on a directory currently being used caused a kernel panic. (CB-9244)

Linux Sensor (5.2.0.160603.1441)

1. Added support for RHEL/CentOS 6.8 version on the endpoint. (CB-9253)

2. Corrected an issue where remote commands executed via Cb Live Response left behind zombie processes. (CB-9236)

Cb Response 5.2.0

Console and Server

1. Corrected an issue where CSV export of hosts that observed a binary in Binary Detail page failed to work if Search Processes page facets were disabled from cb.conf. (CB-4073)
2. Corrected an issue where count of hosts displayed on Dashboard page did not correlate with the value displayed on the Sensor Details page. (CB-4042)
3. Corrected an issue where bulk resolve of more than 1000 alerts did not resolve all alerts on the Triage Alerts page. (CB-4031)
4. Fixed an issue where search links in Watchlist page failed if the search term for the watchlist contained forward slashes. (CB-7275)
5. Corrected an issue where Cb Live Response registry query command failed to return results for registry hives with spaces in them. (CB-3730)
6. Corrected an issue where nightly cron job for tagging documents that match newly added feed reports failed with a KeyError. (CB-7472)
7. Corrected an issue where the searches for time based process document fields showed incorrect syntax under “Showing Results for…” link on the UI. (CB.7724)
8. Fixed an issue where startup script for setting SELinux security context on a NFS share causing startup failures. (CB-3765)
9. Corrected an issue where feed tags associated with a process event erroneously deleted when process document was split into multiple files in the SOLR database. (CB-8346)
10. Fixed an issue where failure to download a file from Carbon Black Alliance Server using cbget when requested file did not exist erroneously reported connectivity to Alliance Server status on the UI as disconnected. (CB-8423)
11. Threat Report create time based searches from the UI now correctly works. (CB-8613)
12. CSV export of events from all search pages are now generated on the server side for robustness. (CB-2826)
13. Triage Alert page is redesigned for cleaner workflow and faster load times. (CB-7548)

14. Sensors page is redesigned for faster load times and ability to page list of sensors within a sensor group for cleaner workflow. (CB-8788)
15. Searches for command lines now correctly works for search terms that contain single quotes. (CB-2807)
16. Process Analyze page preview now correctly renders if process is missing process name or path. (CB-4956)
17. Notes are now retained correctly if a hash is unbanned. (CB-5113)
18. Resolved inconsistency in the Action button functionality on sensor detail and sensor list pages. (CB-5130)
19. Improved Watchlist Name edit functionality. (CB-4913)
20. Added a visual cue for facets selected when no search results are return to improve workflow. (CB-5189)
21. Directory (path) facet on Process Analyze page now correctly displays terms for Linux sensors. (CB-4642)
22. Now sharing settings can be configured while creating a new sensor group. (CB-5471)
23. Corrected an issue where default values for various settings on the sensor group dialog were not reflected correctly. (CB-7529)
24. Watchlist page sidebar now correctly persists sort order after item selection. (CB-7277)
25. “E-mail Me on Hit” option from Watchlist page now works correctly. (CB-7388)
26. Threat Reports page no longer erroneously display deleted reports for manually added feeds. (CB-7416)
27. Watchlist page tooltips now correctly disappear when cursor is moved away from the selection. (CB-7532)
28. Corrected an issue where the Sensors page did not load correctly when a user with access rights to a customer group did not have permissions to default sensor group. (CB-8320)
29. Sensor Group Settings dialog now correctly handles team names with longer than 23 characters. (CB-7629)
30. Tooltips that contain quotes are now handled correctly in Triage Alerts page tooltips. (CB-7679)

31. Confirmation dialog for network isolation now more accurately inform users on the actions/limitations of this feature. (CB-8228)
32. Binary Search page UI now correctly allows wildcard searches in filename field. (CB-7735)
33. SMTP server names that contain hyphen now can be correctly entered in e-mail settings. (CB-8330)
34. Server UI client application now is prevented from running inside another frame. (CB-8432)
35. Process Analyze page now correctly removes spinner when page is rendered. (CB-8886)
36. Watchlist page correctly displays the “last hit” time when there are positive hits to the query. (CB-8957)
37. Corrected an issue where some feed tags were erroneously removed from the process instances when such event data from such processes were split over multiple SOLR documents. (CB-8346)

Windows Sensor (5.2.0.160518.1524)

1. Fixed an issue that caused system crash if the sensor was running on a VM that was going through live migration. (CB-7158)
2. GPO installer now have correct product version. (CB-6953)
3. Sensor core driver can cause system crash if installation fails for any reason. (CB-6929)
4. Sensor can associate wrong parent information to processes which it did not see start (sensor was installed on a running system.) (CB-6911)
5. Sensor can associate wrong start up context to processes which it did not see start (sensor was installed on a running system.) (CB-6873)
6. Sensor service can leak memory on system that are under heavy load (seeing high volume of process execution and termination events.) (CB-7065)
7. Sensor cbstream driver can cause softlock on boot or shutdown on Google Cloud Platform. (CB-6977)
8. Corrected an issue where MSI installer failed re-installation. (CB-7372)

9. Sensor stealth mode installation fails if sensor process name provided does not have .exe extension. (CB-7609)
10. Sensor service may cause network shares to disconnect or otherwise fail when accessing files (CB-7764)
11. Sensor uninstall from web UI fails if sensor name is changed under stealth mode. (CB-8291)
12. Corrected an issue where sensor cbtdiflt driver cause system crash when accessing buffers in chained receive handlers. (CB-8245)
13. Fixed an issue where DNS cache in sensor service was not being populated correctly. (CB-8407)
14. Fixed an issue where cbtdiflt driver was causing system crash due to access to pointers without checking their validity (CB-7718)
15. [New Feature] Sensor now implements suppression of eventless (uninteresting) processes. (CB-7266)
16. [New Feature] Sensor now suppresses known DLLs in Windows process executions when enabled per sensor group. (CB-7294)

Linux Sensor (5.2.0.160518.1322)

1. Fixed an issue where network connection events were associated with incorrect parent process under load. (CB-8214, CB-8485)
2. Fixed an issue where network connection events did not have process path in the raw protobuf events similar to Windows platform, impacting monitoring of raw events from the enterprise event bus. (CB-9045)
3. Cb Live Response on Linux sensor now correctly accesses directories with apostrophes in their name. (CB-9024)
4. Corrected an issue that caused system crash when sensor is put in isolation mode. (CB-8236)
5. Corrected an issue where some process events were missing process PID information. (CB-8748)
6. Corrected an issue where cbdaemon initialization script referred to a directory that no longer exists. (CB-8467)

7. Sensor no longer reports username after user context event collection option is disabled. (CB-8419)
8. Sensor now correctly updates sensorsettings.ini file values received from the server. (CB-8424)
9. Corrected an issue where sensor driver sporadically crashed sending health alert level 75 (driver failure) to the server. (CB-6700)'
10. [New Feature] Sensor now implements suppression of eventless (uninteresting) processes. (CB-7266)
11. [New Feature] Sensor now differentiate between process forks and other executions. (CB-6756)
12. Fixed an issue where putting sensor in network isolation caused it to go offline. (CB-9295)
13. Corrected an issue where installer placed an unexpected file under /opt/cbsensor following install. (CB-9079)

OS X Sensor (5.2.0.160518.1339)

1. OS X sensor now correctly updates sensorsettings.ini file values received from the server. (CB-6463)
2. OS X sensor sensordiag.sh diagnostic script now does not collect log and diagnostic directories that are not pertaining to its operation when packaging diagnostic information. (CB-7785)
3. Corrected an issue in PSC_fork call in OS X sensor causing a kernel panic in process tracking. (CB-6476)
4. Corrected an issue in parsing of DNS packets that caused high CPU usage. (CB-8394)
5. Corrected an issue that caused up to 6 seconds delay in starting applications on a sensor that did not yet check-in with the server. (CB-8885)
6. Sensor no longer reports its own events from CbOsxSensorService. C(B-8840)
7. Corrected an issue where exceptions in protobuf library causing sensor daemon to crash randomly. (CB-6486)

8. [New Feature] Sensor now implements suppression of eventless (uninteresting) processes. (CB-7266)
9. [New Feature] Sensor now differentiate between process forks and other executions. (CB-6564)
10. Added process md5 to child process execution event message protobuf headers. This is useful when parsing raw events on the enterprise message bus for third party analysis. (CB-9446)

Carbon Black Enterprise Server 5.1.1 Patch 4

Console and Server

1. Added sensor interface and communication IP addresses to syslog notifications for Query-based Feed hits. (CB-10536)
2. Fixed an issue with syslog messages using the CEF format template due to incorrect escaping of some characters. (CB-10274)

Windows Sensor (5.1.1.160913.1023)

1. Added support for Windows 10 Anniversary edition. (CB-10591)
2. Fixed an issue where network driver for legacy Windows XP/Windows 2K support caused system crash due to incorrect handling of buffers. (CB-10964)
3. Fixed an issue with third party application conflict with “Imaging for Windows 4.0 by Global360”. (CB-10963)
4. Addressed an issue with excessive boot time when sensor is installed on endpoints with several other security and management tools that all run on startup. (CB-10990)

OS X Sensor (5.1.1.160915.1527)

1. Added support for OS X 10.12 Sierra version. (CB-10540)
2. Removed warnings from logging when getting sensor version from CLI. (CB-10984)
3. Addressed an issue where a memory leak in CreateVnodePath caused memory to be exhausted causing kernel panic. (CB-10959)

4. Optimized sensor efficiency when computing eventlog queue quota sizes. (CB-10962)
5. Fixed an issue where sensor became unresponsive and lost network connectivity while under heavy load. (CB-10957)

Linux Sensor (5.1.1.160913.1004)

1. Fixed an issue with due to malformed ZIP causing binary files downloaded from UI to be corrupt. (CB-10548)
2. Fixed an issue with accessing files on an NFS share that caused system crash. (CB-10993)
3. Fixed an issue where binary file store location under /var/lib/cb/store grew past configured limits. (CB-10992)

Cb Response 5.1.1 Patch 3

Console and Server

1. Changed requests from datastore to use POST method rather than GEt when querying for feed reports so that long report ids can be accommodated without hitting URL limits. (CB-9635)
2. Improve ingress matching for domain name based IOCs to matching on subdomains in addition to the FQDNs, e.g. an IOC domain *example.com* would now match both a network connection to *a.example.com* and *b.example.com.* (CB-7478)
3. UI now correctly honors use_proxy and validate_server_cert options correctly when adding a custom feed. (CB-9649)
4. Server now uniquely identifies alerts generated on ingress feed hits (e.g. from feed hit events feed.hit.ingress.process and feed.hit.ingress.binary) from alerts generated by the feed_searcher cron job nightly runs. While the former alerts only on new process executions or binary reports that match a given feed report, the latter also creates an alert when there is a change in the feed report content or score since the last time a process or binary was tagged. Alerts generated from feed_searcher cron job now have specific alert type that refers to “feedsearch” in name and are displayed in Triage Alerts page with yellow exclamation marks instead of red for easy visual differentiation (CB-9393)

5. UI now asynchronously requests facet data on all search requests instead of only when visiting a search page the first time, reducing the time it takes to load them. (CB-9797)

Windows Sensor (5.1.1.160603.1529)

1. Fixed an issue where sensor service's attempt to access files on network shares as SYSTEM was causing problems with various DFS shares, ranging from corrupted file writes to disconnected share drives. (CB-7764)
2. Corrected a potential issue where sensor service caused divide-by-zero exception. (CB-6839)
3. Corrected an issue where legacy TDI filter driver was accessing pointers without checking if they are valid. (CB-7718)
4. Corrected a slow memory leak that occurred when sensor service is under heavy load. (CB-7065)
5. Corrected a rare bugcheck that occurred in the cbk7.sys sensor driver. (CB-9328)

OS X Sensor (5.1.1.160603.1506)

1. Child process terminated events now correctly report the timestamp of end event, rather than the start event. (CB-9357)
2. Improved DNS parsing code to avoid high CPU usage. (CB-8394)
3. Sensor service no longer reports itself and its child processes to the server. (CB-7534)
4. Fixed an issue that caused sensor service crash in DNS parsing library. (CB-8798)
5. Corrected an issue where remote commands executed via Cb Live Response left behind zombie processes. (CB-9193)
6. Corrected an issue where force umount on a directory currently being used casued a kernel panic. (CB-9244)
7. Sensor now correctly reports CNAMEs in network connection events. (CB-9549)

Linux Sensor (5.1.1.160603.1515)

1. Corrected an issue where sensor service failed to start on reboot following an upgrade. (CB-8864)

2. Netconn events now contain process path as part of the protobuf message headers like in Windows platform. This is useful when parsing raw events on enterprise message bus for 3rd party analysis. (CB-9045)
3. Corrected a slow memory leak that caused elevated memory usage over long periods of time. (CB-9134)
4. Corrected an issue where remote commands executed via Cb Live Response left behind zombie processes. (CB-9236)
5. Added support for RHEL/CentOS 6.8 version on the endpoint. (CB-9253)

Cb Response 5.1.1 Patch 2

Console and Server

1. Corrected an issue where binary file store synchronization cron job was inserting incorrect MD5 hash values into PostgreSQL and therefore was never synchronizing correctly with files stored on disk. (CB-8750)
2. Added ability to broadcast raw sensor eventlogs to api.rawsensordata RabbitMQ exchange. (CB-7330)
3. Incoming network connection events that are tagged as feed hits now correctly shows up as feed hits in the Process Analyze page. (CB-7513)
4. CB Tamper feed hits are now correctly shown in Process Analyze page. (CB-8826)
5. Corrected an issue where Alliance feed hit tags were not correctly copied over when SOLR documents for long-lived processes split into multiple segments causing hit information to be lost. (CB-8346)

Windows Sensor (5.1.1.160415.1734)

1. Corrected an issue where eventlogs were sent to the wrong minion in clustered environment when a CB Live Response session was initiated. (CB-8486)
2. Corrected an issue where last eventlogs were not written to disk upon power off of endpoint causing some events occurring right before shutdown event to be lost. (CB-8420)
3. Fixed an issue that caused core driver to bugcheck in error path during initialization. (CB-8903)

OS X Sensor (5.1.1.160415.1724)

1. Fixed a memory corruption in network connection tracking that caused a crash. (CB-8785)
2. Fixed a memory leak in sensor user space service code. (CB-8740)
3. Fixed a memory leak in sensor kernel extension code. (CB-8802)
4. Fixed a sensor crash due to a failure to map a file to memory. (CB-8410)
5. Added process path and process MD5 to the header of network connection eventlogs uploaded by sensor. This is useful if raw sensor events are broadcast on RabbitMQ bus for archiving or further analysis. (CB-8924)
6. Fixed a spelling mistake in sensor uninstaller output. (CB-8720)

Linux Sensor (5.1.1.160415.1732)

1. Addressed memory leak in cbdaemon on RHEL 7.1/CentOS 6.7 (CB-8444)
2. Added process path and process MD5 to the header of network connection eventlogs uploaded by sensor. This is useful if raw sensor events are broadcast on RabbitMQ bus for archiving or further analysis. (CB-8924)
3. Added event timestamp to the header of process start eventlogs uploaded by sensor. This is useful if raw sensor events are broadcast on RabbitMQ bus for archiving or further analysis. (CB-8551)
4. Fixed an issue that resulted sensor driver to fail after install. (CB-8313)
5. Fixed a kernel panic that was result of a NULL pointer being dereferenced in kernel space. (CB-8754)

Cb Response 5.1.1 Patch 1

Console and Server

1. Corrected an issue where query of feed reports into memory for ingress matching could take a long time and cause data ingest to stop due to small default database paging size of 100. Paging size is now configurable via cb.conf (CB-7487, CB-8287)

2. Corrected an issue with cbinit script failing to create “cb” service user when it is ran as a non-root user. (CB-7545)

3. Corrected an issue with cbinit script failing to locate iptables if it is not in the running user’s PATH variable. (CB-7622)

4. Corrected an issue where cb-enterprise daemon does not successfully re-connect to RabbitMQ message bus if RabbitMQ socket temporarily goes down. (CB-8216)

5. cb-solr service throws UnknownHostException on feed hits if server hostname can’t be resolved causing feed hits to not to be reported. (CB-8218)

6. Corrected an issue where failure to download a file using the command line utility cbget causes Carbon Black Alliance Server communication status to show failure, even though server communication is intact. (CB-8423)

7. If a non-root user has been added to cluster.conf during *cbcluster add-node*, changes to this user in cluster.conf are not reflected in subsequent ssh communication with minions causing other *cbcluster* commands to fail. (CB--7571)

8. Corrected sensorsettings.ini file values for eventlog disk quota percentage and absolute size which were inadvertently reversed. (CB-8387)

9. Corrected an issue with CB API usage where passing an empty string as a sort parameter into a query API caused search to fail. (CB-7351)

10. Corrected an issue with *binary metadata* index purge script command line parsing that caused -g option to not to be honored when in dry-run mode. (CB-4578)

11. Corrected an issue with CBLR execfg command incorrectly parsing its arguments. (CB-7779)

12. Corrected an issue with UI dialog for ignoring future alerts from a feed not appearing when alerts are resolved as false positive. (CB-7640)

13. Corrected tooltips that were not correctly escaped for binary hashes banned from the UI. (CB-8380)

14. Corrected incorrect sizing of process icons in Search Processes page. (CB-7768)

15. Corrected incorrect reference to documentation in VDI sensor group settings. (CB-7547)

16. Modified the feature to filter out sensors that are dormant or inactive. Instead of pruning them from the database, they are now filter at the API level to preserve the historical context of process activity stored by the server. The configuration option in cb.conf has

also been modified to reflect the change in implementation (see section under server upgrade topic.) (CB-4096)

Windows Sensor (5.1.1.160314.0129)

1. Fixed an issue with sensor service frequency computation that caused intermittent “divide-by-zero” errors that resulted in system crash. (CB-8533)
2. Corrected a memory leak in core driver that only occurred if all event collections were disabled. (CB-6969)
3. Corrected an issue in sensor TDI driver (for Windows XP and Windows server 2003) that caused a bug check by accessing pointers without checking if they were valid. (CB-8520)
4. Corrected an issue in sensor TDI driver that caused a bug check due to incorrect handling of chained receive buffers. (CB-8521)
5. Corrected an issue where sensor missed process events generated close to endpoint shutdown due to a missing flush to disk in shutdown path. (CB-8524)
6. Corrected an issue where sensor uninstall from the UI failed when service name has been changed for obfuscation. (CB-8519)

OS X Sensor (5.1.1.160314.0122)

1. Fixed an issue with excessive memory usage on CbOsxSensorService due to incorrect tracking of some processes where sensor did not see the process start (e.g. because service was restarted after). (CB-8230)
2. Fixed an issue with excessive debug messages printed to /var/log/system.log by the sensor. (OS-8227)
3. Fixed a kernel panic under 10.11.2 due to changes to underlying OS kernel structures. (CB-7408)
4. Fixed an issue where some of the child process terminate messages were not reported to the server. (OS-8487)

Linux Sensor (5.1.1.160314.0136)

1. Fixed an issue with excessive memory usage on cbdaemon due to incorrect tracking of some processes where sensor did not see the process start (e.g. because service was restarted after). (CB-8314)
2. Corrected an issue where cbdaemon stopped working after some time and a status check on it returned “cbdaemon is dead but subsys locked”. (CB-8371)
3. Fixed an incorrect reference to a directory path during cbdaemon initialization script. (CB-8386)
4. Fixed an issue that caused sensor to post CBLR commands incorrectly. (CB-7510)
5. Corrected an issue that caused sensor to hang under heavy system load. (CB-6650)

Carbon Black Reponse 5.1.1

Console and Server

1. Improved logging in feed synchronizer background task. (CB-3932)
2. Corrected an issue with sensor uninstall from the UI when user does not have global administrator privileges. (CB-4006)
3. Improved logging in feed synchronizer background task. (CB-3932)
4. Corrected an issue with sensor uninstall from the UI when user does not have global administrator privileges. (CB-4006)
5. Resolved a race condition between SQL purge maintenance task and Alliance Server binary uploads. (CB-4008)
6. Updated nginx cb-multihome.conf.example to match the nginx cb.conf that is shipping in 5.1. (CB-4012)
7. Fixed incorrect time stamps on sensor communication failures. (CB-4014)
8. Corrected misleading cb.conf content. (CB-4016)
9. Resolved emails not being sent for host-based Tamper Detection events issue. (CB-4020)
10. Fixed failures in moduleinfo_insert statements because of an integer overflow in

primary 'id' sequence on the SQL table. (CB-4028)

11. Fixed an issue with bulk resolve of alerts due to a logic error in API calls. (CB-4035)
12. Fixed an issue with alerts from OSX/Linux 4.x sensors that resulted in invalid process links. (CB-4037)
13. Fixed an issue with redundant syslog events from feed searcher job every time a MD5 matches a feed. (CB-4045)
14. Corrected invalid report id errors from watchlist searcher. (CB-4048)
15. Fixed an issue persistence of global feed alert settings on the UI across multiple users. (CB-4058)
16. Corrected an issue with total blocks counter not being updated for banned hashes. (CB-4059)
17. Corrected an issue with ignore status on feed report being nullified on feed full-sync. (CB-4062)
18. Corrected an issue with cbcluster start hangs while CbTools continues to run. (CB-4065)
19. Corrected an issue with disabling "Process user context" event collection not being reflected in the systemsettings.ini file. (CB-4066)
20. Removed sensor purge functionality in favor of filtering Sensor Details page results in the API. (CB-4069)
21. Added parent_unique_id field to the results returned by the rest API search() endpoint. (CB-4074)
22. Fixed an issue with Process Analyze page feed facets. (CBUI-1036)
23. Corrected a discrepancy in sensor queue values reported by UI versus the rest API. (CBUI-1130)
24. Corrected “Email Me” option not being persisted after watchlist creation issue. (CBUI-1532)
25. Corrected an issue with "Export All to CSV" action on Sensors page failing to export all sensors. (CBUI-1575)
26. Improved how drag and drop on "team settings" UI page works. (CBUI-1576)
27. Search Binaries page now correctly displays "ago" in the first-seen field on result rows.

(CBUI-1578)

28. Corrected an issue with incorrect search being performed when clicking on “Publisher” field in Process Analyze page. (CBUI-1582)
29. Corrected an issue on selection of a facet for process analysis. (CBUI-1600)
30. Corrected an issue with “sensor filter by node” facet, which resulted in incorrect selections on the Sensors page. (CBUI-1601)
31. Fixed an issue with hyperlinks on UI notifications drop down. (CBUI-1602)
32. Improved sensor "yield" tooltip messaging when the issue is health score related. (CBUI-1612)
33. Corrected an issue with custom threat feed dialog not correctly disappearing after adding a feed url manually. (CBUI-1686)

Windows Sensor (5.1.1.151030.0948)

1. Fixed an issue with kernelSocketConnect in cbk7.sys that resulted in system crash in some machines. (WIN-306)
2. Fixed a potential memory leak in cbtdiflt close completion handling. (WIN-340)
3. Fixed an issue with sensors not honoring "collect binaries" checkbox in sensor group settings. (WIN-349)
4. Fixed an issue with sensor dropping network connections on Win 2K3 endpoints. (WIN-352)
5. Resolved an issue that resulted in sensors not communicating to server on isolate. (WIN-360)
6. Resolved a potential deadlock due to holding FAST_MUTEX while calling ZwSetValueKey(). (WIN-362)

OS X Sensor (5.1.1.151217.0244)

1. Sensor now correctly rotates/expunges log files so that /var partition is not filled. (OSX-251)
2. Reduced excess error events in system.log with OS X 10.11. (OSX-281)

Linux Sensor (5.1.1.151215.1153)

1. Sensors now correctly rotate/expunge log files so that /var partition is not filled. (LNX-194)
2. Sensor now correctly honors Binary/Eventlog collection limits (1GB or 2% each) with small partitions. (LNX-196)
3. Fixed a kernel panic on systems running *named* linux service. (LNX-206)

Cb Response 5.1.0 Patch 3

Console and Server

1. Fix file permissions for /etc/cb/cb_ssh so that it is not readable except by root user. (CB-3645)
2. Updated /api/user/<name>/permissions API call to check requester's team membership before returning permissions information for users. (CB-3692)
3. Fixed e-mail actions so that notifications are sent for host-based tamper detection events. (CB-4020)
4. Corrected an issue with negation of Alliance-based feed fields in process searches. (CB-4033)
5. Corrected an issue with IP address searches with CIDR ranges broader than /8. (CB-4044)
6. Fixed an issue where a previously *ignored* feed report's status is nullified after feed-sync action. (CB-4062)
7. Disabled caching of HTTPS responses by browser clients. (CB-4655)
8. Corrected an issue where deleting all watchlists caused the Watchlist page to fail. (CB-4995)
9. Corrected an issue where resolving an alert failed if alert name contained ">" character. (CB-5026)
10. Corrected an issue in behavior of *sensor -n* command in CB Live Response session. (CB-5176)

11. Corrected an issue where some complex queries failed due to improperly encoded POST request by the API. (CB-7241)

12. Corrected an issue where escaping a colon in text-based queries resulted in a failed request. (CB-7252)

13. Corrected an issue where a watchlist search link failed if the query terms included forward slashes. (CB-7275)

Windows Sensor (5.1.0.151215.1242)

1. Fixed an issue where turning off all event collections resulted in memory leak and instability in the core Carbon Black driver. (CB-6969)

Linux Sensor (4.2.9.151215.0933)

1. Added support for RHEL/CentOS 7.2. (CB-7376)

Cb Response 5.1.0 Patch 2

Console and Server

1. Corrected a behavior where throttle_calc task in cb-enterprise uses progressively more CPU. (E-4698)
2. Fixed an issue with OS process document count in alliance statistics are broken in clustered deployments. (E-4688)
3. Updated nginx cb-multihome.conf to match nginx cb.conf in the product shipping with 5.1. (E-4669)
4. Corrected an issue with feed_searcher sending to syslog every time a md5 matches a feed to include VirustTotal. (E-4652)
5. Added logic to rate-limit number of binary hash check HTTP calls to prevent self-inflicted denial of service on the cb-datastore. (E-4697)
6. Corrected an issue with cbdiag --post failing when post size is “too large” in some customer environments. (E-4668)
7. Corrected an issue with watchlist searcher throwing “Invalid Report ID” error causing current job to fail. (E-4677)
8. Fixed the system hang due to CbTools background task is running in the system cbcluster. (E-4646)

Windows Sensor (5.1.0.150911.0926)

1. Fixed an issue with CB 5.1.0 sensor upgrades failing if service is renamed (obfuscation) but core driver is not. (WIN-346)
2. Fixed a potential memory leak in cbtdiflt “connection close/completion” handling. (WIN-340)
3. Fixed a system crash issue when doing a live migration of a VM host. (WIN-329)

Linux Sensor (4.2.8.150908.0431)

1. Corrected a kernel panic in systems running Linux named service. (LNX-206)

Linux Sensor (4.2.9.151002.1507)

This is sensor adds support for Linux 6.7. It is not generally available. Please contact Bit9 + Carbon Black Technical Support team to get access.

Cb Response 5.1.0 Patch 1

Console and Server

1. CentOS 6.7 fails requesting to upgrade python-urllib3 library. This issue has been addressed in this release. (E-4612)
2. Addressed a failure when cb-enterprise services are started, due to cb-redis service no longer being able to create its own PID file. This is because SELinux policy in CentOS 6.7 has changes that restrict Redis process to where it is allowed to write PID and log files. (E-4653).
3. Several changes were made to increase the security of Carbon Black. (CBUI-1216)
4. Tagged processes could lose their highlighting in the console when they were later shown in search results. This issue has been fixed in the patch. (CBUI-1224)
5. URLs that directly referenced a console page would first open the login page and then display the Welcome page instead of the page referenced in the URL. In this release, the user is directed to the correct page after authentication. (CBUI-1386)
6. Process or binary search boxes now accept a comma-separated list of query fields. (CBUI-1502)
7. Fixed an issue where the UI would occasionally display 504 errors, timeout errors or the license graph not being displayed after an upgrade from earlier releases to version 5.1.0. (E-4094)

8. Addressed an issue where the Watchlist page was blank if a proxy was configured for the server. (E-4334)
9. Inactive sensors are now removed after 10 days of inactivity. (ENT-4409)
10. Corrected an issue where the EventPurgeEarliestTime date in cb_settings is being set in the future. This prevented deletion of files that should have been purged, which caused unnecessary disk usage. (E-4457)
11. Addressed performance issues, especially with backlog processing. (E-4506)
12. Corrected an issue where the binary downloads failed in clusters using a non-standard API port. (E-4508)

Windows Sensor (5.1.0.150805.0434)

1. Fixed an issue where Chkdsk would not run on reboot when Carbon Black sensor was installed on certain Windows operating systems. (WIN-314)

Cb Response 5.1.0

Console and Server

1. Administration/Sensors page takes a long time to load on Servers with large number of sensors. (CBUI-1236)
2. Addressed some non-functioning CBLR Commands on FireFox. (CBUI-1285)
3. UI does not allow non-global-admin administrator of a group to edit group settings, the issue has been addressed in this release. (CBUI-1307)
4. Fixed the Binary Preview hyperlink search it was not returning any results. (CBUI-1385)
5. If you click on the notification boxes in a threat intelligence feed (the available boxes are "create alert" and "log to syslog"), the boxes will remain checked for the user who checked them, but they will not appear checked for other users. This issue has been addressed. (CBUI-1437)
6. Fixed the Watchlist Email Me option as when changed by 1 user, it affected other users. (CBUI-1448)
7. When performing a process search by date, CB 5.0 will return search results for the prior day's data. The issue has been addressed. (CBUI-1402)
8. Address the issue where the server was reaching maximum number of DB connection in a clustered environments. (E-3835)
9. After an alert has been resolved from the Triage Alerts page’s default query, and the page is reloaded the alert shows unresolved again. This issue has been fixed. (E-3838)

10. Server dashboard does not display on occasion due to a product issue. The displayed error was: "unable to add db connection back to pool". This issue has been fixed. (E-3852)
11. The cbcluster startup performance issue has been addressed for this release. This issue appears after upgrading to 5.0.0 Patch 2. (E-4002)
12. Server scripts are displaying the following error <gevent.dns.DNSError'>: [Errno 67] request timed out. (E-4190)
13. If an exception is thrown during a full feed sync via the command line, all work appears to stop. The issue has been fixed. (E-4200)
14. Observing constant stream of HTTP 500 errors in the NGINX. The issue has been addressed by the server having a background health check task that monitors activity and log any time there is a SQL transaction that runs for a long time. (E-4210)
15. The purge process is not processing all appropriate files, which causing excessive disk usage. This issue has been addressed. (E-4235)
16. Triage alert is getting triggered repeatedly for the same file from the same endpoint even after it was acknowledge. The issue has been addressed in this release. (E-4290)
17. CSV generation from the process analyze view results in empty filemods.csv and regmods.csv. This is even if the result on the console shows entries for filemods and regmods events. The issue has been addressed in this release. (E-4382)
18. SSO setting is not redirecting with the specified port. (E-4388)

Windows Sensor (5.1.0.150618.0432)

1. CB Live Response “kill” command now works correctly on Windows 8+ machines when attempting to kill a process not running in the same session as cb.exe (typically session 0). (WIN-304)
2. Upgrade failure messages are now correctly sent to the server when upgrades failed. (WIN-144)
3. Improved accuracy of binary storefile backlog reporting. (WIN-199)
4. Modload event collection now can be correctly disabled. (WIN-235)
5. Fixed an issue with false positive tamper events sent related to sensor’s own activity on startup and shutdown. (WIN-300)
6. Fixed a race condition where persisted events may have been lost if another application on the system happened to have the file open when the sensor tried to send the events. (WIN-297)

7. Fixed an issue with operation of CB Live Response that prevented it to start after clean install of sensor. (WIN-296)
8. Reduced the likelihood of CB sensor's hashing and binary inspection to cause sharing violations with other applications' binaries. (WIN-290)
9. Fixed an issue with sensor uninstaller not removing the "HKLM\software\wow6432node\carbonblack" registry key on 64-bit systems. (WIN-297)
10. Improved reporting of delayed writes that occurred after a process has exited. (WIN-279)
11. Fixed an issue on Windows 7+ machines that led to cb.exe to have high CPU utilization. (WIN-277)
12. Improved agents debouncing logic to avoid sending duplicate module info events to the server. (WIN-276)
13. Corrected reporting of cross-process events on Windows XP and 2003 systems when one process successfully performed a CreateRemoteThread operation. (WIN-274)
14. Fixed a small race condition on driver unload that could lead to memory leak or in rare cases a system crash. (WIN-265)
15. Fixed an issue with very long registry paths causing system to crash. (WIN-264)
16. Improved accuracy of byte counts of outstanding uploads that is reported to the server. (WIN-262)
17. Fixed an issue that causes events that were in queue to be lost when the sensor service was stopped. (WIN-259)
18. Fixed an issue that caused sensor to report multiple ntoskrnl.exe (SYSTEM) processes for the same boot session with slightly different process creation times. (WIN-250)
19. Fixed an issue that caused binary information of running processes to not be collected If binary info collection is disabled and then re-enabled. (WIN-248)

OS X Sensor (4.2.7.150624.0430)

1. A race condition in the daemon would occasionally cause it to crash. This has been corrected. (OSX-209).

Linux Sensor (4.2.7.150624.1613)

1. The Linux sensor now gracefully handles DNS timeouts. (LNX-98).
2. An issue was fixed involving RPM name collision of the Linux sensor installer package installed on the cb-enterprise server. (LNX-137).
3. Support for Redhat/Centos 7.1 has been added. (LNX-144).

4. The Linux sensor will now ignore its own operations. (LNX-152).
5. The subsystem start/shutdown sequence was adjusted to avoid a potential race.

Known Issues and Limitations

5.2.x Linux sensor paravirtualization support

The 5.2.x Linux sensor cannot currently run on VMs hosted by the Xen Hypervisor in paravirtualization (PV) mode. We have seen issues in such environments because paravirtualized hosts do not behave the same as the Operating Systems they emulate. This issue will be addressed in a future release.

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 (e.g. module loads) or some features might be unavailable (e.g. 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.

Changes to nginx configuration directory

Customers upgrading to 5.2.0 from earlier versions will find that nginx proxy configuration directory (/etc/cb/nginx/conf.d) layout has changed in this version. Custom nginx server configuration that is contained in cb.server.custom file is now located under /etc/cb/nginx/conf.d/includes. Customers may need to edit their nginx cb.conf file to update the include path of this file to reflect the new directory hierarchy following the upgrade.

For additional troubleshooting information and configuration examples, see the following knowledgebase articles:

https://community.carbonblack.com/docs/DOC-5430

https://community.carbonblack.com/docs/DOC-5441

Installations Using Single Sign On

Customers upgrading to 5.1.1 Patch 2 from earlier releases may need to edit their SSO configuration file to ensure proper operation after upgrading. The following steps should be taken:

1. Verify the name of the current sso configuration file being used. This is defined in /etc/cb/cb.conf with the SSOConfig parameter, e.g.:
   `SSOConfig=/etc/cb/sso/sso.conf`
2. In the sso configuration file, find the entry for the assertion_consumer_service. It will look similar to the following:

```
"endpoints": {
          "assertion_consumer_service": [
            [
              "https://<IP Address>/api/saml/assertion",
             "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
            ]
          ]
  },
```

3. If the assertion_conumer_service is defined using square-bracket syntax as in the example above, change it to use curly-brace and replace the comma to a colon in its syntax, as follows:

```
      "endpoints": {
      "assertion_consumer_service": {
            "https://<IP Address>/api/saml/assertion":
           "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
       }
},
```

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, e.g. 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, e.g.

```
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 workaround this shortcoming, the logical OR could be translated into a logical AND by using the equivalent negated version of the entire query, e.g. 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, e.g.

```
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.

Automatic pruning of inactive sensors

In version 5.1.0 Patch 1, we have added configuration logic to prune out sensors that are dormant or inactive. This would include systems that are offline, uninstalled or otherwise not communicating with the Cb Response server for a given number of days. The following configuration has been added to the cb.conf file to control pruning of such inactive sensors:

```
DeleteInactiveSensors=True
DeleteInactiveSensorsDays=10
```

By default the value is set to *False*.

In 5.1.1 Patch 1, we modified the configuration to filter out sensors that are dormant or inactive, rather than pruning them from the database to preserve the historical context of process activity stored by the server. The configuration option in cb.conf has also been modified to reflect the change in implementation:

```
SensorLookupInactiveFilterDays
```

If this value is unset (default), all sensors are returned. When SensorLookupInactiveFilterDays set to > 0, only sensors that checked in the past SensorLookupInactiveFilterDays days will be returned.

Important Note:

Users upgrading to 5.1.1 Patch 1 or Patch 2 from earlier releases may need to update their cb.conf file to reflect this change. ***The new setting supersedes both previous settings and the legacy settings are ignored by the system****.*

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, we recommend 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 can not 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 Support

For your convenience, Carbon Black Technical Support offers several channels for resolving support questions:

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

Reporting Problems

When you call or e-mail Carbon Black Technical Support, please provide the following information to the support representative:

Required Information	Description
Contact	Your name, company name, telephone number, and e-mail 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