Summary

CB Response 6.3.0 is a feature release of the CB Response server and console. 6.3.0 release contains new features, enhanced permissions, and SHA256 visibility, in addition to bug fixes, better supportability, and performance improvements.

The 6.3.0 version of the server adds CentOS and RHEL 7.6 qualifications [CB-22812].

These release notes include the following information:

- Enhanced Permissions Changes
- SHA256 Visibility
- Queries with Modloads Performance Improvement
- Document Contents
- [On-Prem Only] Preparing for Server Installation or Upgrade
- Configure Sensor Updates Before Upgrading Server
- New Feature: Enable CB Live Response setting
- New Feature: Endpoint for IP Address Whitelisting
- New Feature: Queries with Modloads Performance Improvement
- Corrective Content
- Known Issues

Enhanced Permissions

CB Response will now have complete Enhanced Permissions feature. Global administrators will have greater control over what users can see in the console. Global administrators can manage user access for CB Response's most powerful features such as Live Response, Host Isolation, Hash Banning, Uninstall Sensor, Tamper Detection. All the permissions are granted on a per-user basis. All backend endpoints are fully secured against calls with invalid permissions.

Enhanced Permissions is supported in Unified View. This version of Unified View is included in this release.

See 6.3.0 User Guide for more details

Link to download current version of Unified View:

```
https://yum.carbonblack.com/unifiedview/6.3.0-2/$releasever/$basearch
/
```

SHA256 visibility

CB Response server will start supporting SHA256 with this release. Users can view and query on SHA256 hashes. SHA256 hash is available in process search, binary search, watchlists, alerts, query feeds and emails. This release does not include hash banning. Banning hashes will still be performed with MD5 hash.

All SHA256 fields are available on cbevents_v2 schema. On upgrade to 6.3.0, the cbevents_v2 schema will become the default schema for cbevents core, so that SHA-256 process fields are available on the console. Built-in functionality in the new server version will ensure that the events core is rolled over so that the schema change will take effect.

WARNING: Please remove `CurrentEventsSchema=cbevents_v1` directive from `/etc/cb/cb.conf` on instances where cbevents_v1 schema was forced, for SHA256 feature to work on the console.

This change will impact on-prem customers only. All cloud customers already have cbevents_v2 schema enabled by default.

This release includes the following components:

- Server version 6.3.0.190301
  Release Notes: (this document)
- Windows Sensor version 6.1.9.181012
  Release Notes
- MacOS Sensor version 6.2.4.190226
  Release Notes
- Linux Sensor version 6.1.10.10169
  Release Notes

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

Document Contents

This document provides information for users who are upgrading to CB Response Server version 6.3.0 from previous versions, and for users who are new to CB Response. The key information specific to this release is provided in the following major sections:

- **Preparing for Server Installation or Upgrade** – Describes requirements to meet and key information needed before beginning the installation process for the CB Response server.
- **New features** – Provides a quick reference to the new and modified features that are introduced with this version.
- **Corrective content** – Describes issues that are resolved by this release as well as more general improvements in performance or behavior.

- **Known issues and limitations** – Describes known issues or anomalies in this version.

Additional Documentation

This document supplements other Carbon Black documentation. Click here to search the full library of CB Response user documentation on the Carbon Black User eXchange.

Technical Support

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

Use one of the following channels to request support or ask support questions:

- **Web:** User eXchange
- **Email:** support@carbonblack.com
- **Phone:** 877.248.9098
- **Fax:** 617.393.7499

Reporting Problems

When contacting Carbon Black Technical Support, provide the following required information:

- **Contact:** Your name, company name, telephone number, and email address
- **Product version**: Product name (CB Response server and sensor version)
- **Hardware configuration:** Hardware configuration of the CB Response server (processor, memory, and RAM)
- **Document version:** For documentation issues, specify the version and/or date of the manual or document you are using
- **Problem:** Action causing the problem, the error message returned, and event log output (as appropriate)
- **Problem severity:** Critical, serious, minor, or enhancement request

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

[On-Prem Only] Preparing for Server Installation or Upgrade

This section describes the requirements and key information that is needed before beginning the installation process for the CB Response server. All on-premises users, whether upgrading or installing a new server, should review this section before proceeding. Next, see the appropriate section of the *CB Response Server/Cluster Management Guide* version 6.3.0 for specific installation instructions for your situation:

- **To install a new CB Response server**, see “Installing the CB Response Server”.
- **To upgrade an existing CB Response server**, see “Upgrading the CB Response Server”.

Yum URLs

CB Response Server software packages are maintained at the Carbon Black yum repository (yum.distro.carbonblack.io). **The links will not work until the on-prem GA date**.

Our yum links for the CB Response server have changed. The following links make use of variables to ensure that you install the correct version of CB Response, based on your machine's OS version and architecture.

Use caution when pointing to the yum repository. Different versions of the product are available on different branches as follows:

- **Specific version:** The 6.3.0 version of server and Unified View is available from the Carbon Black yum repository specified in the following base URLs:

  Server:

  ```
  baseurl=https://yum.distro.carbonblack.io/enterprise/6.3.0-2/$releasever/$basearch/
  ```

  Unified View:

  ```
  baseurl=https://yum.carbonblack.com/unifiedview/6.3.0-2/$releasever/$basearch/
  ```

  This link is available as long as this specific release is available. It can be used even after later versions have been released, and it can be useful if you want to add servers to your environment while maintaining the same version you already have installed.

- **Latest version:** The latest supported version of the CB Response server and Unified View is available from the Carbon Black yum repository specified in the following base URLs:

  Server:

  ```
  baseurl=
  https://yum.distro.carbonblack.io/enterprise/stable/$releasever/$basearch/
  ```

  Unified View:

  ```
  baseurl=https://yum.carbonblack.com/unifiedview/stable/$releasever/$basearch/
  ```

This will point to version 6.3.0-2 until a newer release becomes available, at which point it will automatically point to the newer release.

Note: 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 can 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 can communicate with standard CentOS yum repositories.

[On-Prem Only] System Requirements

Operating system support for the server and sensors are listed here for your convenience. The document *CB Response Operating Environment Requirements* document describes the full hardware and software platform requirements for the CB Response server and provides the current requirements for systems that are running the sensor. This document is 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 Operating Environment Requirements before proceeding.

Server / Console Operating Systems

Note: For best performance, Carbon Black recommends running the latest supported software versions.

- CentOS 6.7-6.10 (64-bit)
- CentOS 7.3-7.6 (64-bit)
- Red Hat Enterprise Linux (RHEL) 6.7-6.10 (64-bit)
- Red Hat Enterprise Linux (RHEL) 7.3-7.6 (64-bit)

Installation and testing are performed on default install 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)

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

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

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

Configure Sensor Updates Before Upgrading Server

CB Response 6.3.0 comes with updated sensor versions. Servers and sensors can be upgraded independently, and sensors can be upgraded by sensor groups instead of 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, and strongly recommends that you review your Sensor group Upgrade Policies before upgrading your server to avoid inadvertently upgrading all sensors at the same time. For detailed information on Sensor Group Upgrade Policy, see the Sensor Group section of the *CB Response User Guide* for version 6.3.0.

To configure deployment of new sensors via the CB Response web UI, follow the instructions in the *CB Response User Guide*.

New features

Enable CB Live Response setting [CB-22139]

Global administrators can enable or disable Live Response on the Advanced Settings page, but only if `CbLREnabled` is removed from cb.conf or commented out. If `CbLREnabled` is present in cb.conf, global administrators cannot change its state on the Advanced Settings page.

Endpoint for IP Address Whitelisting [CB-22138]

Cloud customers can now whitelist IP addresses via /whitelist endpoint. See developer site for documentation.

Queries with Modloads Performance Improvement [CB-14781]

Prior CB Response server releases have reported that some process queries that join with event fields (such as modload) are slow. Follow these guidelines to get better results.

Take note of any event fields included in your query (such as modload, regmod, filemod, etc.). When more than one expression containing one of these fields is a part of an AND query, or any field is negated with NOT, it will trigger a join subquery. Event metadata fields (such as process_name, etc.) can be part of the query and will never trigger join subqueries.

To optimize a query containing multiple event fields combined with AND, always put the part of the query that will return the most documents first before any other expressions containing event fields. They should also come before negated expressions containing event fields.

For example, consider the following 3 separate queries:

- modload:rare (returns 1000 documents)
- modload:common (returns 10,000,000 documents)
- modload:lesscommon (returns 100,000 documents)

The optimal way to write a query that ANDs these together is:

modload:common AND modload:rare AND modload:lesscommon

Alternatively, the query

modload:common AND modload:lesscommon AND modload:rare

is exactly the same from a performance perspective. The benefit of reordering fields consists of placing the part with the most results before parts with fewer results.

Note that process metadata fields, such as process_name, are not subject to this issue. Metadata fields are handled very efficiently in SOLR.

Corrective Content

1. When creating a new team, by default the sensor groups have Analyst role access only. [CB-22702]
2. After 6.3.0 server fresh install, the Administrators Team has "Administrator" (Analyst) role permissions for the Default Sensor Group. [CB-22645]
3. A user with no group/team will not have access to do anything except to view the Profile page. The user will not be presented with any UI to navigate. A user with roles that have the correct permissions will not receive any errors from the API. [CB-18518]
4. APIs that retrieve CBLr sessions will not time-out when there are many expired sessions. New parameters are added to the endpoint to return active or inactive sessions.

   Calls to api/v1/cblr/session (GET) with the new parameter active_only=true will return only the active sessions.

   Calls to api/v1/cblr/session (GET) with active_only=false, or with active_only not included, will return all sessions.

   You can specify floating point values for CbLrDefaultSessionTTLDays (e.g. CbLrDefaultSessionTTLDays=0.01). The thread that deletes the session data will run hourly, so deletion can occur one hour past the specified time interval.

   Deletion of expired sessions will run without an exception any time it finds an expired session [CB-20837],[CB-20632]

Known Issues

1. Invalid query when creating a watchlist from a Threat Feed. When creating a watchlist from a Threat Feed, CB Response incorrectly creates the query and the watchlist will not run and creates an error. To see if your watchlist that was created from a threat feed has formed an error, check the Watchlist page for the status. As a workaround, the CB Response Team suggests clicking on the Search Binaries or Search Process hyperlinks on the Threat Feed and then Add/Create Watchlist action from the search page.
2. If the browser timezone is different from the server timezone, you might notice a discrepancy in the last check-in time shown for Sensors. [CB-20076]
3. The CSV export of the user activity audit is malformed in certain cases. [CB-18936]
4. The CSV Export of ‘Recently Observed Hosts’ has no header row. [CB-18927]
5. When using a custom email server, you cannot enable or disable Alliance Sharing. The workaround for this is to disable the custom email server, make the change, then re-enable customer email server. [CB-20565]
6. For sensor upgrades to work properly, you might need to configure McAfee EPO to exclude `c:\windows\carbonblack\cb.exe` from its "Prevent creation of new executable files in the Windows folder" option. [CB-7061]
7. Command Line query hyperlink in Process Analyse page is not working if the command line begins with a leading forward ‘/’. Leading forward ‘/’ is not tokenized, and is treated as a command line switch. Alternatively use `cmdline:usr/sbin/netbiosd` or `cmdline:“usr/sbin/netbiosd”` in the search to get results. [CB-25072]