Carbon Black.

Cb Response

Release Notes

Version 6.2.1

March 2018

Carbon Black, Inc.

1100 Winter Street, Waltham, MA 02451 USA

Tel: 617.393.7400 Fax: 617.393.7499

Email: support@carbonblack.com

Web: http://www.carbonblack.com

Introduction

The *Cb Response 6.2.1 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 – Describes preparations you should make before beginning the installation process for Cb Response server.
- Upgrading the Cb Response Server – Provides information and instructions specific to server upgrades.
- New and Modified Features – Provides a quick reference to the new and modified features introduced with this version.
- Corrective Content – Describes issues resolved by this release as well as more general improvements in performance or behavior.
- Known Issues and Limitations – Describes known issues or anomalies in this version that you should be aware of.
- Contacting Carbon Black Support – Describes ways to contact Carbon Black Technical Support, and it details what information to have ready so that the technical support team can troubleshoot your problem.

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

Purpose and Contents of this Release

The Cb Response 6.2.1 release contains new sensor versions, bug fixes, and stability and performance improvements. It packages the following component versions:

- Server version – 6.2.1.180130.1054
  Release Notes: (this document)
- Windows Sensor version – 6.1.2.71109
  Release Notes: https://community.carbonblack.com/docs/DOC-9772
- macOS Sensor version – 6.1.3.80124
  Release Notes: https://community.carbonblack.com/docs/DOC-9773
- Linux Sensor version – 5.2.13.71018
  Release Notes: https://community.carbonblack.com/docs/DOC-10153

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

Documentation

The standard user documentation for the Cb Response product includes:

- *Cb Response User Guide* – Describes Cb Response feature functionality in detail, plus administrative functions.
- *Cb Response Server/Cluster Management Guide* – Describes how to install, manage, backup/restore, etc. a Cb Response server/cluster. This guide is for on-premises Cb Response installations only.
- *Cb Response Server Sizing Guide* – Provides details on infrastructure sizing for Cb Response server.
- *Cb Response Server Configuration Guide (cb.conf)* – Describes the contents of the cb.conf file, the primary configuration file for Cb Response. By changing the values of parameters in cb.conf, you can change the behavior and performance of Cb Response.
- *Cb Response API* – Documentation for the Cb Response API is located at https://developer.carbonblack.com.

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

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 Server/Cluster Management Guide* for version 6.2.
- **To upgrade a Cb Response server**, see Upgrading the Cb Response Server later in this document.

Yum URL

Cb Response Server software packages are maintained at the Carbon Black yum repository (yum.distro.carbonblack.io). Use caution when pointing to the yum repository; different versions of the product are available on different branches as follows:

- **Specific version:** The 6.2.1 version described here is available from the Carbon Black yum repository specified in the following base URL:
  baseurl= https://yum.distro.carbonblack.io/enterprise/6.2.1-1/x86_64/
  This link will remain available as long as this specific release is available. It can be used to get to this release even after later versions have been released, and so 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 is available from the Carbon Black yum repository specified in the following base URL:
  baseurl= https://yum.distro.carbonblack.io/enterprise/stable/x86_64/
  This will point to version 6.2.1-1 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 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.

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

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

- CentOS 6.7-6.9 (64-bit)
- Red Hat Enterprise Linux (RHEL) 6.7-6.9 (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)

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

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

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

Technical Support

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

Upgrading the Cb Response Server

Supported Upgrade Paths

Server upgrades to 6.2 are supported from the following previous versions:

- All 5.1.*x* versions, including earlier patch releases
- All 5.2.*x* versions, including earlier patch releases
- All 6.*x* versions, including Early Access Program (EAP) and Controlled Distribution releases

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

Important: Ports and protocol requirements in version 6.*x* have changed since version 5.*x*. Refer to the "Ports and Protocols" chapter of the *Cb Response Server/Cluster Management Guide* for details.

Configure Sensor Updates Before Upgrading Server

Cb Response 6.2 comes with updated sensor versions. If you are upgrading your server, decide if you want 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.

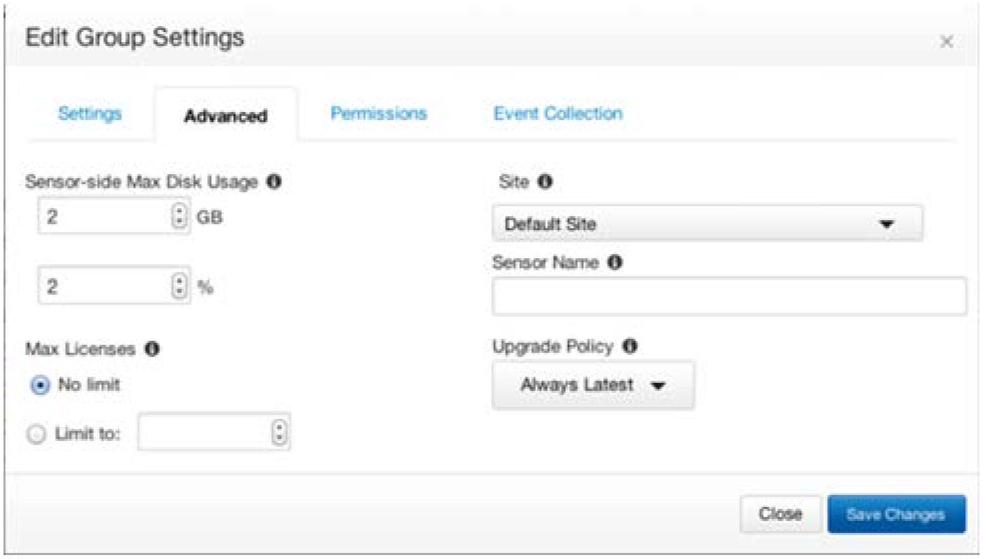
Decide if you would like the new sensor to be deployed immediately to existing sensor installations, or if you want to install only the server updates first. Carbon Black recommends a gradual upgrade of sensors to avoid any unacceptable impact on network and server performance.

Note: *There is no expected degradation to sensor performance with Cb Response 6.2.1.*

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

Versions 5.1.1 and Below:

1. Log into the console, navigate to the Sensors page, and edit the group settings for each active Sensor Group:



Edit Group Settings

Sensor-side Max Disk Usage: 2 GB

2 %

Max Licenses: ● No limit ○ Limit to:

Site: Default Site

Sensor Name:

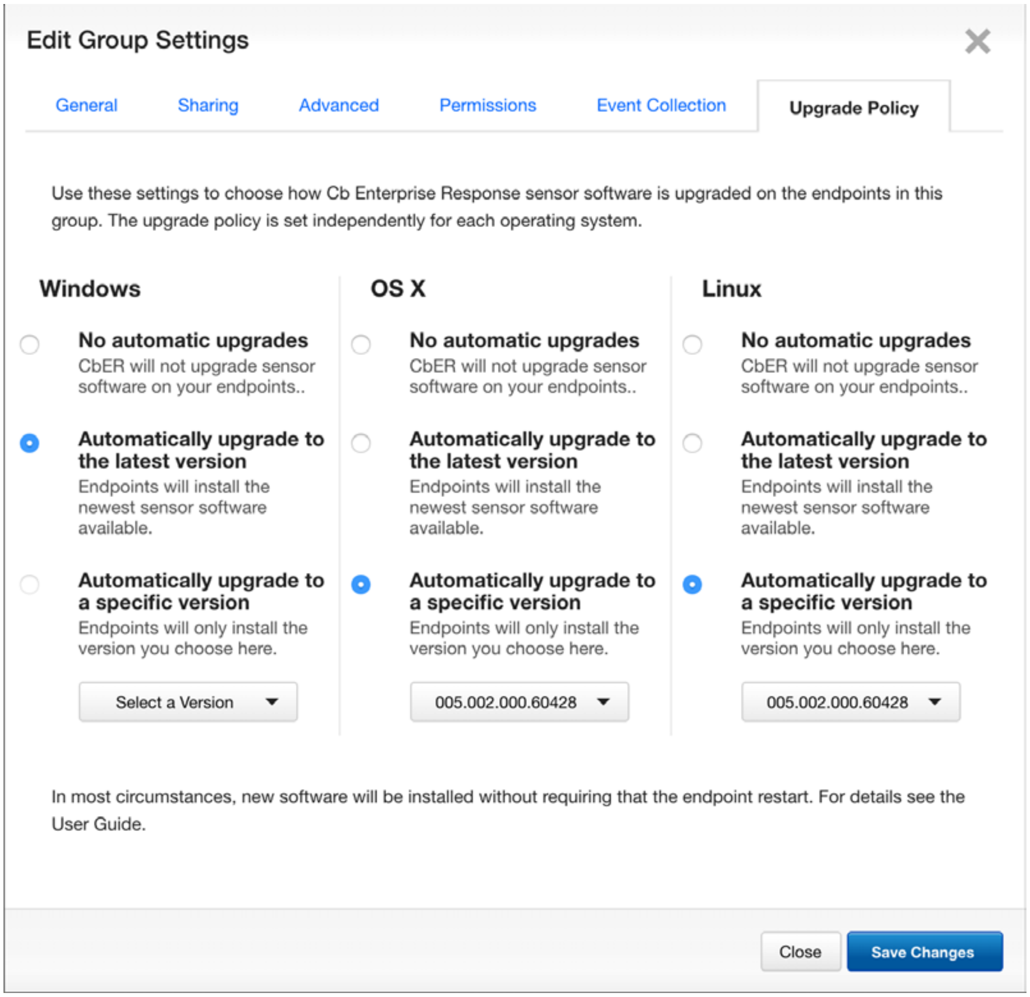
Upgrade Policy: Always Latest

2. 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:

1. Log into the console, navigate to the Sensors page, and edit the group settings for each active Sensor Group:



Edit Group Settings

Use these settings to choose how Cb Enterprise Response sensor software is upgraded on the endpoints in this group. The upgrade policy is set independently for each operating system.

Windows

○ **No automatic upgrades** CbER will not upgrade sensor software on your endpoints..

● **Automatically upgrade to the latest version** Endpoints will install the newest sensor software available.

○ **Automatically upgrade to a specific version** Endpoints will only install the version you choose here.

Select a Version ▾

OS X

○ **No automatic upgrades** CbER will not upgrade sensor software on your endpoints..

○ **Automatically upgrade to the latest version** Endpoints will install the newest sensor software available.

● **Automatically upgrade to a specific version** Endpoints will only install the version you choose here.

005.002.000.60428 ▾

Linux

○ **No automatic upgrades** CbER will not upgrade sensor software on your endpoints..

○ **Automatically upgrade to the latest version** Endpoints will install the newest sensor software available.

● **Automatically upgrade to a specific version** Endpoints will only install the version you choose here.

005.002.000.60428 ▾

In most circumstances, new software will be installed without requiring that the endpoint restart. For details see the User Guide.

2. Under the Upgrade Policy tab, find the platform type you want 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.
    a. To keep the sensors at a specific version, select that version number from the drop-down list prior to upgrade.
    b. 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 must 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 release of Cb Response includes the following changes in functionality:

- Audit logging can now be made to include API calls in the audit activity. This is configurable by setting `EnableExtendedApiAuditLogging=True` in the cb.conf file.
- The Sensors page in the console has been redesigned for a more user-friendly appearance.
- Apache Solr in the Cb Response server has been upgraded to version 5.5.5.

Corrective Content

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

1. Improved memory encoding for API responses larger than 50 Mb. (CB-15652)
2. Using negated binary terms for a process search should now return proper results. (CB-13935)
3. Console has been sanitized for potentially malicious HTML elements hidden in command lines. (CB-16164)
4. Improved performance for the Banning page in the Cb Response console. (CB-14840)
5. Improved usability for New Search Terms dialog box for process search. Can now enter a negative value for **in the last n minutes** when specifying a new search term using **Time > Start time**. (CB-16112)
6. When adding a user, input for username input is now validated and limited to 256 characters. (CB-16128)
7. For non-root use of the `cbcluster add-node` command, added two commands to the list of those required in the sudoers file (`cbupgrade --check` and `cbupgrade --non-interactive`). These were missing in earlier releases of the 6.2 user documentation. See the “Using CBCLUSTER as a Non-Root User” chapter in the “Cb Response Server/Cluster Management Guide” for the full sudoers example. (CB-18348)

Known Issues and Limitations

Sensors Pages Chrome Browser Limitation

The redesigned Sensors page is compatible only with Chrome browser versions 54 and higher.

OS X Sensor Upgrade Limitation

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

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

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

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

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

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, for example:
   `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, for example, A OR -B.

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

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

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

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

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

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

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

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

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

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

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 cannot be disabled on Linux platforms. (CB-6686)
10. On OS X platforms, the UI setting to turn all “event collections” off is not honored. (CB-6389)
11. Binary execution of a file can still be banned if the file reuses the same inode on Linux and OS X platforms. (CB-6647/CB-6402)
12. If a sensor’s system clock is wrong and in the future, the start time for processes from that sensor are not displayed correctly in the Carbon Black console. (CB-6257)
13. On the Carbon Black server, when a sensor is moved out of a group with a user on a team that has only "Viewer" access to that particular group, results for that group are still searchable for the time period it was in that group, but the Process Details page links get 405 errors. If the sensor is put back into the group, the 405 errors for those processes go away. (CB-3704)
14. The Reshard tool can fail with “File Not Found” exception, in turn causing a corrupt index. If a re-shard is necessary please contact support for a potential work around. (CB-3743)
15. The Linux sensor fails to properly cache observed events after the disk quota is reached and connection to the server is lost. (CB-6722)
16. The Linux sensor may fail to generate an MD5 and collect a binary image of file on a network share or user-space file system. (CB-6749)
17. CbEP enforcement fails after the Linux Sensor is uninstalled. A restart of CbEP is required to restore enforcement. (CB-7674)

Contacting Carbon Black Support

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

Technical Support Contact Options
Web: www.carbonblack.com/support/
Email: support@carbonblack.com
Phone: 877.248.9098
Fax: 617.393.7499

Reporting Problems

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

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