

## Summary

VMware Carbon Black EDR 7.5.2 is a maintenance release of the VMware Carbon Black EDR (formerly CB Response) server and console. This release delivers bug fixes.

See the [Corrective Content](#) section for more details.

This release notes document includes the following sections:

- [Document Contents](#)
- [\[On-Prem Only\] Preparing for Server Installation or Upgrade](#)
- [Configure Sensor Update Settings Before Upgrading Server](#)
- [Corrective Content](#)
- [Known Issues](#)
- [Contacting Support](#)

This release includes the following components:

- Server version 7.5.2.211028  
[Release Notes](#) (this document)
- Windows Sensor version 7.2.2.17680  
[Release Notes](#)
- MacOS Sensor version 7.2.0.16495  
[Release Notes](#)
- Linux Sensor version 7.0.3.15300  
[Release Notes](#)
- (Legacy) Windows Sensor version 6.1.13.15392  
[Release Notes](#)
- (Legacy) Linux Sensor version 6.3.4.10012  
[Release Notes](#)

Each release of VMware Carbon Black EDR software is cumulative and includes changes and fixes from all previous releases.

# Document Contents

This document provides information for users who are upgrading to VMware Carbon Black EDR Server version 7.5.2 from previous versions, and for users who are new to VMware Carbon Black EDR and are installing it for the first time.

The key information specific to this release is provided in the following major sections:

- **[On-Prem Only] Preparing for Server Installation or Upgrade** – Describes requirements to meet and information needed before beginning the installation process for the VMware Carbon Black EDR server.
- **Configure Sensor Update Settings Before Upgrading Server** –
- **New Features** – Provides a quick reference to new and modified features that are introduced in this version.
- **Corrective Content** – Describes issues that are resolved by this release, and general improvements in performance or behavior.
- **Known Issues** – Describes known issues or anomalies in this version.
- **Contacting Support** – Describes ways to contact Carbon Black Technical Support and what information to have ready.

# Additional Documentation

This document supplements other Carbon Black documentation. Supplemental release documentation can be found in the new [Carbon Black EDR section of docs.vmware.com](https://docs.vmware.com/en/Carbon-Black-EDR), rather than on the VMware Carbon Black User Exchange, where release documentation used to be published.

In addition to this document, you should have access to the following key documentation for VMware Carbon Black EDR Server 7.5.2:

- *VMware Carbon Black EDR 7.5 User Guide*: Describes how to use the Carbon Black EDR servers that collect information from endpoint sensors and correlate endpoint data with threat intelligence.
- *VMware Carbon Black EDR 7.5.1 Server / Cluster Management Guide*: Describes installation, configuration, and upgrade of Carbon Black EDR servers.
- *VMware Carbon Black EDR 7.5 Unified View Guide*: Describes the installation and use of the VMware Carbon Black EDR Unified View server. Information on server hardware sizing requirements and software platform support is included.

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

This section describes the requirements and key information that is needed before installing a VMware Carbon Black EDR server. All on-premises users, whether upgrading or installing a new server, should review this section before proceeding. See the appropriate section of the *VMware Carbon Black EDR 7.5.1 Server / Cluster Management Guide* for specific installation instructions for your situation:

- **To install a new VMware Carbon Black EDR server**, see “Installing the VMware Carbon Black EDR Server”.
- **To upgrade an existing VMware Carbon Black EDR server**, see “Upgrading the VMware Carbon Black EDR Server”.

### Customers on Server 5.x, please note:

Direct upgrades from Server 5.x to Server 7.x *are not* supported. Please refer to Page 31 of the *VMware Carbon Black EDR 7.5.1 Server / Cluster Management Guide* and this [VMware Carbon Black User Exchange announcement](#) for more information.

## Yum URLs

VMware Carbon Black EDR Server software packages are maintained at the Carbon Black yum repository ([yum.distro.carbonblack.io](https://yum.distro.carbonblack.io)). The links will not work until the on-prem General Availability (GA) date.

The following links use variables to make sure you install the correct version of VMware Carbon Black EDR, based on your machine's operating system 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 7.5.2 version is available from the Carbon Black yum repository, that is specified in the following base URL:

baseurl= [https://yum.distro.carbonblack.io/enterprise/7.5.2-1/\\$releasever/\\$basearch](https://yum.distro.carbonblack.io/enterprise/7.5.2-1/$releasever/$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.

- **Latest version:** The latest supported version of the VMware Carbon Black EDR server is available from the Carbon Black yum repository, that is specified in the following base URL:

baseurl= [https://yum.distro.carbonblack.io/enterprise/stable/\\$releasever/\\$basearch/](https://yum.distro.carbonblack.io/enterprise/stable/$releasever/$basearch/)

This URL will point to version 7.5.2-1 until a newer release becomes available, at which time it will automatically point to the newer release.

**Note:** Communication with this repository is over HTTPS and requires appropriate SSL keys and certificates. During the VMware Carbon Black EDR 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 a mirror from which to download the dependency packages. If a VMware Carbon Black EDR server is installed behind a firewall, local network and system administrators must make sure that the host machine can communicate with standard CentOS yum repositories.

## [On-Prem Only] System Requirements

Operating system support for the server and sensors is listed here for your convenience. The *VMware Carbon Black EDR 7.5 Operating Environment Requirements* document describes the full hardware and software platform requirements for the VMware Carbon Black EDR server and provides the current requirements and recommendations for systems that are running the sensor.

Both upgrading and new customers must meet all of the requirements specified here and in the *VMware Carbon Black EDR 7.5 Operating Environment Requirements* document before proceeding.

## **Server / Console Operating Systems**

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

- CentOS 6.7 - 6.10 (64-bit)
- CentOS 7.3 - 7.9 (64-bit)
- CentOS 8.1 - 8.3 (64-bit)
- Red Hat Enterprise Linux (RHEL) 6.7 - 6.10 (64-bit)
- Red Hat Enterprise Linux (RHEL) 7.3 - 7.9 (64-bit)
- Red Hat Enterprise Linux (RHEL) 8.1 - 8.4 (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.

However, if the customers are pinning dependencies to a specific OS version, the product only supports the following software versions for the Carbon Black EDR Server and Unified View:

- CentOS 6.7 - 6.10 (64-bit)
- CentOS 7.5 - 7.9 (64-bit)
- CentOS 8.2 - 8.3 (64-bit)
- Red Hat Enterprise Linux (RHEL) 6.7 - 6.10 (64-bit)
- Red Hat Enterprise Linux (RHEL) 7.5 - 7.9 (64-bit)
- Red Hat Enterprise Linux (RHEL) 8.2 - 8.4 (64-bit)

**Note:** Versions 7.3, 7.4, and 8.1 (64-bit) of CentOS/RHEL are not supported if customers are pinning dependencies.

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 current list of supported operating systems for VMware Carbon Black EDR sensors, see <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 Update Settings Before Upgrading Server

VMware Carbon Black EDR 7.5.2 comes with updated sensor versions. Servers and sensors can be upgraded independently, and sensors can be upgraded by sensor groups.

Decide whether you want the new sensor to be deployed immediately to existing sensor installations, or install only the server updates first. Carbon Black recommends a gradual upgrade of sensors to avoid network and server performance impact. We strongly recommend 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 *VMware Carbon Black EDR 7.5 User Guide*.

To configure the deployment of new sensors via the VMware Carbon Black EDR web console, follow the instructions in the *VMware Carbon Black EDR 7.5 User Guide*.

## Corrective Content

1. EDR Server 7.5.2 introduces an improved event tokenizer that is designed to improve data ingestion. This new tokenizer is disabled by default, but can be enabled and configured via the Cb Events v2 Schema, which is located at:

```
/etc/cb/solr/core_conf/configsets/cbevents_v2/conf/schema.xml
```

The new tokenizer is to be used in place of (not in addition to) the original tokenizer mechanism. To use the new tokenizer, replace the references to the original tokenizer, 'CbEventsTokenizerFactory', with 'CbEventsTokenizerFactoryNG' in `/etc/cb/solr/core_conf/configsets/cbevents_v2/conf/schema.xml` on all nodes in a cluster.

Alternatively, execute:

```
sed -i  
's/CbEventsTokenizerFactory/CbEventsTokenizerFactoryNG/g'  
/etc/cb/solr/core_conf/configsets/cbevents_v2/conf/schema.xml on  
all nodes in a cluster.
```

To revert back to the original tokenizer, replace the references to the new tokenizer, 'CbEventsTokenizerFactoryNG', with 'CbEventsTokenizerFactory' in /etc/cb/solr/core\_conf/configsets/cbevents\_v2/conf/schema.xml on all nodes in a cluster.

Alternatively, execute:

```
sed -i  
's/CbEventsTokenizerFactoryNG/CbEventsTokenizerFactory/g'  
/etc/cb/solr/core_conf/configsets/cbevents_v2/conf/schema.xml on  
all nodes in a cluster.
```

[CB-36505]

## Known Issues

1. Beginning in Server 7.4.2, on the Search Threat Reports page, searching for a range of IP addresses (Add Criteria > IP address > enter a range of network addresses) is broken. The query attempt will repeat indefinitely but never successfully complete until the user forces it to stop or closes the browser. [CB-35676]
2. Beginning in Server 7.5.0, the export of Process Analysis events does not work properly for an export of a large number of events (> ~50). If a user clicks on the 'Actions' drop-down and clicks 'Export events', with ~50 or more events selected, the CSV export will contain no data or very limited, incomplete data. This issue was introduced in Server 7.5.0. [CB-35675]
3. Beginning in Server 7.5.0, on the Triage Alerts Page, an invalid search with malformed syntax fails silently, without an error message. In previous versions, an invalid query would return an error message of "Malformed syntax in search query." Via the API, a malformed query submitted on Server 7.5.0 or 7.5.1 returns a 500 error with no error message, whereas a malformed query submitted on previous versions returns a 400 error with the "Malformed syntax in search query." error message. [CB-35669]
4. Beginning in Server 7.5.0, in the Configure Watchlist Expiration panel on the Watchlists page, a whole number must be entered for the watchlist expiration duration in order to save, even when the first option, "Do not mark watchlists as expired if they have no hits." is selected. The configuration should successfully save when "Do not mark watchlists as expired if they have no hits." is selected and the "Notify me when watchlists have not received hits in" value is blank. [CB-35668]

5. Beginning in Server 7.5.0, a user with “No Access” to a particular sensor group will experience an infinite loading indicator on the Live Query page when they try to execute a Live Query that includes that sensor group. [CB-35335]
6. Beginning in Server 7.5.0, when clicking on a link in the header of the Process Analysis page to go to the corresponding Process Search result, the Process Search does not execute automatically upon entering the Process Search page. The user has to click the “Search” button for the Process Search to execute, which is a new behavior. [CB-35313]
7. Beginning in Server 7.5.0, when using the `GET/v1/process/{guid}/{segmentid}/preview` API, process information is not properly returned. [CB-35148]
8. Beginning in Server 7.5.0, when using the `GET /v3/{guid}/event` API (or `GET /v5/{guid}/event`), submitted child process events of type "2" (other exec) do not properly store the process PID. [CB-35147]
9. Beginning in Server 7.5.0, Binary Search searches can sometimes return zero results when there are matching results that should be returned. [CB-35139]
10. Beginning in Server 7.4.0, in the Process Analysis events list, “Crossproc” events that are marked with the tamper flag should also display a red dot, like other tamper events, but they do not. Also, in Process Search, there should be a red dot in the process’ Hits column for a process that has a tamper flag, but there is not. [CB-34964]
11. Beginning in Server 7.3.0, on the Process Search page, a process that has a Threat Intelligence Feed hit tag in one segment may not display the feed hit icon (a red dot) when “Group by process” is selected. [CB-33586]
12. In some cases, a process Watchlist will produce more hits than alerts. When a Watchlist query is executed using the original terms (e.g. `process_name:notepad.exe`), both the original segment (with events) and the tagged segment (without events) are returned, and both results appear on the Watchlists page. This makes it appear that there have been two hits, when in fact, there was only one. The result is two apparent hits, but only one alert, which is deceptive. [CB-33355]
13. `cb-enterprise` fails to install on RHEL/CentOS 8 with FIPS 140-2 enabled, which is due to a change in Red Hat 8 that affected Paramiko ([https://bugzilla.redhat.com/show\\_bug.cgi?id=1778939](https://bugzilla.redhat.com/show_bug.cgi?id=1778939)). The workaround is to use RHEL/CentOS 7 if you enable FIPS 140-2. [CB-33352]
14. Live Query fails to take the `SensorInactiveFilterDays` setting into account when determining which sensors to target. The sensor count on the right side of the ‘Current query’ bar shows all targeted sensors, while the quantity of targeted sensors in the ‘Run



New Query' pop-up does account for `SensorInactiveFilterDays`, and will sometimes show a lower number. [CB-31136]

15. For Server versions 6.x.x - 7.2.0 (all versions which include Apache Solr 6.x), a bug in Apache Solr 6 (<https://issues.apache.org/jira/browse/SOLR-9882>.) causes incomplete results when `partialResults=True`. The Pagination bar, together with a large number, will appear on the Process Search page as a result of a search. However, only a few or even zero actual documents are displayed. [CB-30074]

The fix for this issue has not yet been validated in Server 7.3.0 +, based on Apache Solr 8.

16. Any modification, creation or deletion of files inside `C:\Windows\CarbonBlack` will create Tamper Alerts with empty "Tamper Type" fields on the Triage Alerts page due to file modifications inside the Windows sensor's working directory. [CB-27698]
17. After an upgrade of server and sensor, older files did not get SHA-256 values. When an older file is executed, it creates a process event that contains SHA-256. When a user clicks the link, the binary store shows no SHA-256. [CB-24519]
18. When using a custom email server, you cannot enable or disable Alliance Sharing. The workaround is to disable the custom email server, make the change, and re-enable the custom email server. [CB-20565]
19. The CSV export of the user activity audit is malformed in certain cases. [CB-18936]
20. The CSV export of **Recently Observed Hosts** has no header row. [CB-18927]
21. For Server versions 6.x.x - 7.1.0, which include Apache Solr 6.x, Process Searches using `*_md5,md5, *_SHA256, SHA256` are case-sensitive. These searches were case-insensitive in pre-6-series Server versions, which include Apache Solr 5.x. [CB-14311]

This issue is resolved in Server 7.1.1 +.

22. When creating a watchlist from a Threat Feed, VMware Carbon Black EDR incorrectly creates the query and the watchlist does not run – it creates an error. To see if your watchlist formed an error, check the status on the Watchlist page. As a workaround, the VMware Carbon Black EDR team suggests clicking the **Search Binaries** or **Search Process** hyperlinks on the Threat Feed, and then using the **Add/Create Watchlist** action from the Search page.

# Contacting Support

VMware Carbon Black EDR server and sensor update releases are covered under the Carbon Black Customer Maintenance Agreement. Technical Support can assist with any issues that might develop. 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](mailto: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 (VMware Carbon Black EDR server and sensor versions)
- **Hardware configuration:** Hardware configuration of the VMware Carbon Black EDR 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 you review the related content on the [User Exchange](#) and the new release documentation location, the [Carbon Black EDR section of docs.vmware.com](#).