# Release Notes: macOS Sensor v7.2.1

November 2021


# Summary

VMware Carbon Black EDR macOS Sensor 7.2.1 delivers Event Exclusions on macOS 11 (Big Sur), support of wildcards in path-based exclusions, support of macOS 12 (Monterey), and various bug fixes and stability improvements.

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

This document provides information for users who are upgrading to VMware Carbon Black EDR macOS Sensor 7.2.1 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:

- **Installation Instructions –** Provides instructions for VMware Carbon Black EDR macOS sensor installation.
- **New Features** – Provides a quick reference to new and modified features that are introduced in 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.

## Server Compatibility

VMware Carbon Black EDR sensors included with server releases are compatible with all server releases going forward. It is always recommended to use the latest server release with our latest sensors to utilize the full feature capabilities of our product, however, using earlier server versions with the latest sensor should not impact core product functionality.

## Sensor Operating Systems

VMware Carbon Black EDR sensors interoperate with multiple operating systems. For the most up-to-date list of supported operating systems for VMware Carbon Black EDR sensors (and all VMware Carbon Black products), refer to the following location in the VMware Carbon Black User eXchange: https://community.carbonblack.com/docs/DOC-7991

## Documentation

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



Carbon Black, Inc. | 1100 Winter Street, Waltham, MA 02451 USA | Tel: 617.393.7400

## Technical Support

VMware Carbon Black EDR 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 assist to ensure a smooth and efficient upgrade or installation.

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

# Installation Instructions

To install the new sensor, please follow the steps below. For unattended installs using an MDM solution, use the following inputs to create profiles for preventing endpoint user prompts. More information can be found at the UeX post here.

Plug-in ID: `com.carbonblack.es-loader`

System Extension Bundle ID: `com.carbonblack.es-loader.es-extension`

Application Bundle ID: `com.carbonblack.CbOsxSensorService`

Apple Team ID: `7AGZNQ2S2T`

To install the sensors on to your server, run through the following instructions:

1. Ensure your VMW CB EDR YUM repo is set appropriately:
    a. The VMW CB EDR repository file to modify is */etc/yum.repos.d/CarbonBlack.repo*
    b. Baseurl = https://yum.distro.carbonblack.io/enterprise/stable/$releasever/$basearch/
2. On the VMW CB EDR server, clear the YUM cache by running the following command:
    a. *yum clean all*
3. After the YUM cache has been cleared, download the sensor install package by running the following command:
    a. Run *yum install --downloadonly --downloaddir=<package local download directory> <package>*
        i. **Note:** The *<package local download directory>* is a directory of your choice
        *ii.* **Note:** *<package>* is replaced by *cb-osx-sensor*
4. Install the new sensor package on the VMW CB EDR server by running the command:
    a. *rpm -i --force <package>*

5. Make the new installation package available in the server console UI by running the command:
    a. */usr/share/cb/cbcheck sensor-builds --update*
        *i.* **Note:** If your groups have *Automatic Update* enabled, the sensors in that group will start to automatically update.

Your new sensor versions should now be available via the console. For any issues, please contact VMware Carbon Black Technical Support.

# New Features

- **Event Exclusions** – macOS Sensor 7.2.1 introduces configurable event exclusions to macOS 11 (Big Sur) - a feature that existed previously for kernel extension-based versions. This feature provides the capability to filter out specific types of events from sensor collection.

- **Support of Wildcards in Path-Based Event Exclusions** – macOS Sensor 7.2.1 introduces the ability to use wildcards (*) to filter out entire paths from event collection, which is an enhancement to the existing capability to filter out specific, individual paths. Wildcards can be used in the middle or end of a path to filter out all folders and/or files contained within.

# Corrective Content

This release provides the following corrective content changes:

- Resolved an issue in which CbDigitalSignatureHelper had high CPU usage. [CB-35141]
- Resolved an issue in which CbOsxSensorService had high CPU usage. [CB-34051]
- Resolved an issue in which installing the sensor on an M1 machine required Rosetta. [CB-36383]
- Resolved an issue in which event counters were not being incremented in sensor_raw_events.log. [CB-35528]
- Resolved an issue in which the sensor reports on its own events. [CB-32943]

# Known Issues and Limitations

Known issues associated with this version of the sensor are included below:

- There are a limited number of features which are not available in this version, but which are intended for future development outside the kernel. These features include and are limited to: Proxy address reporting.

- Disabling the collection of file modifications within the Event Collection settings of a Sensor Group in the UI does not actually disable the collection of file modifications by the sensor(s) within that group. [CB-37529]

- When content filters are installed and enabled or uninstalled and disabled, existing connections are terminated. This is by design per Apple. [CB-32640]

- The EDR macOS Sensor does not store Live Response activity in the *sensor.log* file by default. Users can monitor Live Response activity using the *live-response.log* found under */var/log/cb/audit* on the EDR server. Additionally, users can enable more verbose logging of the *sensor.log* file to capture Live Response activity on the Mac endpoint. **Please note**, enabling verbose logging may quickly consume the specified *sensor.log* size and should be used cautiously as enabling may lead to shorter retention of audit information. This verbose logging can be enabled by modifying the *logging.config* file under */var/lib/cb* to to set the following parameters: *minloglevel: 0*, *V:0*. [CB-8908]
- Uninstallation of the sensor should be done via the Server. Manual uninstallation via Terminal will require the user password to be entered. This is by design per Apple. [CB-32640]

# Contacting Support

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 VMware Carbon Black Technical Support, be sure to provide the following required information about your question or issue:

- **Contact:** Your name, company name, telephone number, and email address
- **Product version**: Product name (VMware Carbon Black EDR server and sensor version)
- **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, error message returned, and event log output (as appropriate)
- **Problem severity:** Critical, serious, minor, or enhancement request