

Carbon Black Cloud sensor version 3.3.4.6 is a generally available maintenance release for macOS only. Sensor version 3.3.4.6 includes full support for macOS Catalina.

In these release notes:

- [Important notification about the certificate whitelist process](#)
- [Release checksums](#)
- [Fixed in this release](#)
- [Known issues and caveats](#)

Important notification about the certificate whitelist process

Devices that are upgrading to 3.3.4 from sensor versions 3.0 and older should have the new code signing certificate (**Team ID 7AGZNQ2S2T**) whitelisted prior to the sensor upgrade. This procedure is required because of a Team ID change in the Carbon Black Cloud code signing certificate that was introduced in the 3.1 sensor release. See the [Known issues](#) section for more details.

VMware Carbon Black recommends using an MDM-compatible mass deployment solution to push the updates, pre-approve, and whitelist the KEXT code signing certificate.

See the following User Exchange article about granting the sensor Full Disk Access as required by macOS 10.14+: [macOS 10.14+ Privacy Changes and Granting the macOS Sensor Access](#).

Release checksums

3.3.4.6 DMG SHA256 Checksum	beba3486dbce19c50f48b73cbafe26b02351171369b87e8232b3707ac43a1a95
3.3.4.6 PKG SHA256 Checksum	f87ec9f6e0dfddc041c4d9402cd4bb96751147bb59cd57e676ea46fb8121afc1

Carbon Black.

Fixed in this release

Efficacy enhancements and bug fixes

Issue ID	Description
DSEN-6575 EA-15150	Resolved an issue that caused macOS endpoints to experience degraded performance and event population latency in the backend.
DSEN-6696 EA-15250	Work around a regression in macOS 10.15.1 concerning Apple's VFS API that, in some hardware configurations, resulted in kernel panics at OS boot/reboot when the macOS sensor was installed.
DSEN-6288	Resolves a LiveQuery issue that resulted in the sensor occasionally entering a loop when it encountered an error while attempting to run a query.
DSEN-6473 EA-15173	Resolved sensor tamper protection false positive triggered during OS reboot that resulted in interop between sensor and OS tools attempting to temporarily disable sensor service. That issue manifested with Alerts and MODIFY_SENSOR TTP.
DSEN-6193 DSEN-6238	General script detection improvements
DSEN-5912 DSEN-6631	Installer fixes for 10.15 Catalina that address issues of failed sensor upgrade and incomplete uninstall

Known issues and caveats

Description
There is a known issue where Malware Removal infrequently and inaccurately reports actions.

Issue ID	Affected Product	Description
DSEN-2735	Carbon Black Cloud	Device name in sensor management is case sensitive.

Carbon Black.

DSEN-2700	Carbon Black Cloud sensor	Rare issue where <code>repmgr</code> service sporadically crashes on shutdown, typically when the cloud is unreachable. The issue has no impact on end-user or product efficacy.
DSEN-2543	Carbon Black Cloud sensor	The unattended install script does not accept multiple long options. The workaround is to always provide a value (such as 0 or 1) next to every long option following = character; for example: <code>--downgrade=1</code> <code>--skip-kext-approval-check=1</code> .
DSEN-3740	Carbon Black Cloud	When a device is removed from an AD domain, the sensor is still reflected within that domain on the Endpoints page and remains in a sensor group. The sensor must be taken out of auto-assignment to make policy updates to that sensor. As a workaround, you can manually remove the sensor from the AD group and assign a policy (click into the device, turn off auto-assign, and change the policy).
DSEN-3752	Carbon Black Cloud	Cloud uninstall of the sensor takes a long time due to a change in the backend.
DSEN-3669	CB Defense	Old canary files, specifically with variable or random file names, are not always properly cleaned up by the sensor. This can cause ransomware false positives.