PSC sensor version 3.3.1.12 is a GA (General Availability) release for macOS only.

In these release notes:

Important

As part of this release, we made the certificate whitelist process more granular and secure. You must reconfigure all certificate whitelists by adding common name strings for the items that are currently whitelisted by ORG strings. See **Efficacy enhancements** in the Fixed in this release section for more details.

Devices that are upgrading from versions **3.0** and older to **3.1**+ 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 CB Defense code signing certificate that was introduced in the 3.1 sensor release. See the Known issues and caveats section for more details. Carbon Black recommends using an MDM-compatible mass deploy solution to push the updates, pre-approve, and whitelist the KEXT code signing certificate.

Release checksums

3.3.1.12 DMG SHA256 Checksum	596e7c14115f275881af4a554505cf0a8a380e32f08a7d7e4efe4e39474a2e82
3.3.1.12 PKG SHA256 Checksum	a890734fcc203894a64a64f5ffc1c0a8a9b0c6829e9e70c4ac1adc2c192ea9de

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

Carbon Black.

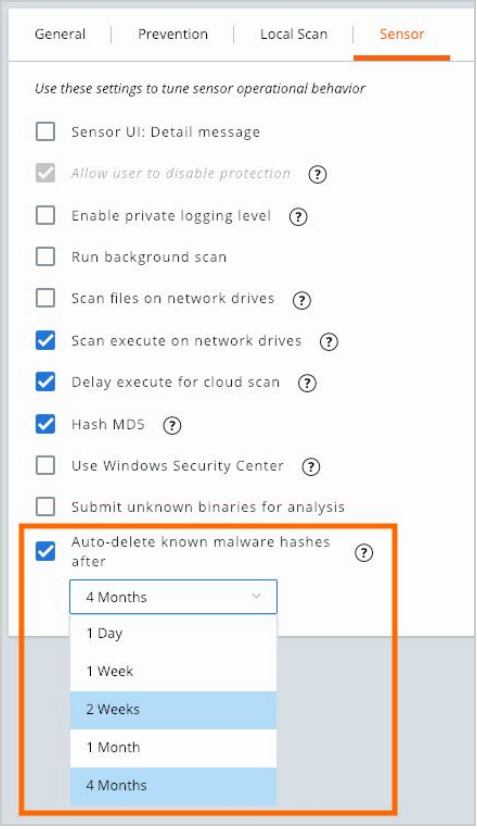
New features

Live Query

Live Query is a new component to Carbon Black's LiveOps product, which is part of the Predictive Security Cloud product suite. CB LiveOps consists of Live Response and Live Query. To enable a device to return Live Query results, your organization must have purchased CB LiveOps and have a 3.3 sensor or later version present on an endpoint. To read more about how to use Live Query, please visit our community. Live Query on macOS is currently running the 3.2.6 version of osquery.

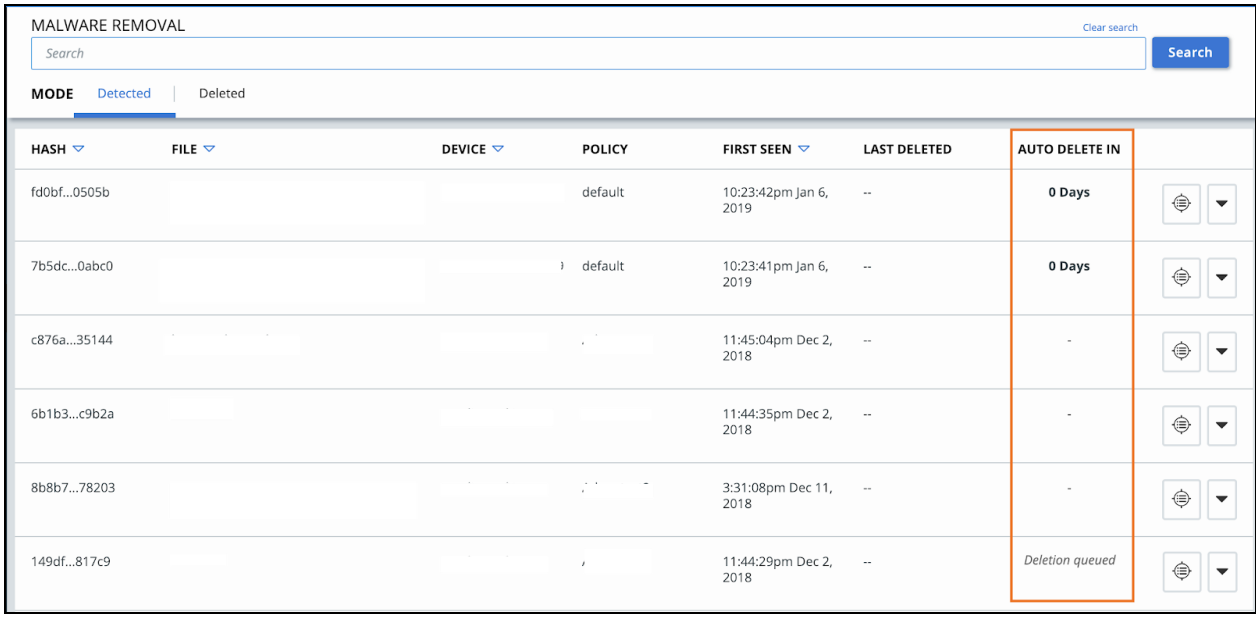
Auto-Delete

The Auto-Delete feature lets you set a time frame during which hashes that are marked as KNOWN_MALWARE are automatically deleted after they are identified on the endpoint. This release achieves parity between the Windows and macOS sensor functionality for the Auto-Delete feature.

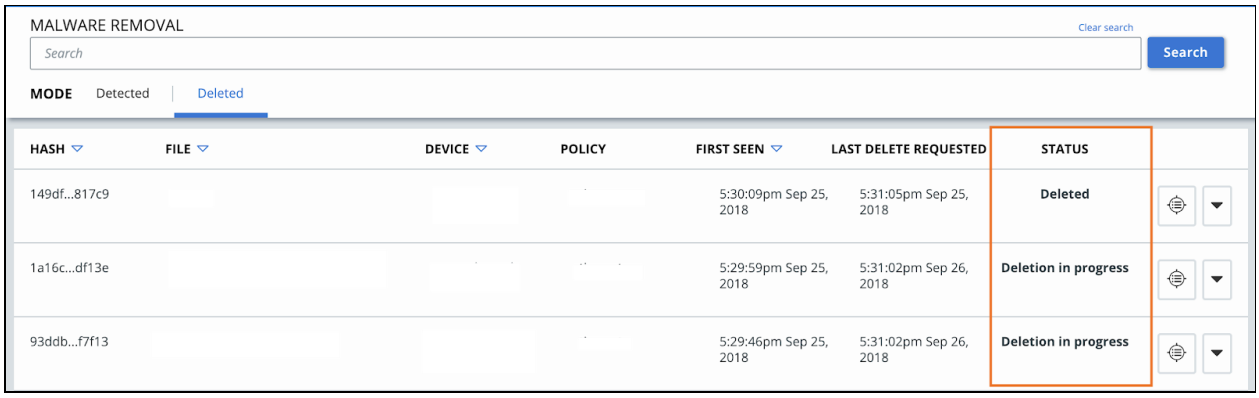


On the **Policies** page under the **Sensor** tab, you can enable the Auto-Delete feature and select a time frame (1 day, 1 week, 2 weeks, 1 month, or 4 months) for when the deletion will occur. Choose the time frame that is most appropriate for your organization to vet for false positives. After a file is deleted, the file is not recoverable.

After KNOWN_MALWARE is identified, the file is immediately quarantined in-place and then deleted after the selected time period elapses. The time frame lets you inspect and investigate the hash before it is deleted. Files that are queued up for Auto-Delete are shown in the **Malware Removal** page under the **Detected** tab. The **Auto Delete In** field reflects the status of the selected time frame.



The file is not backed up and any deletion is permanent. The history of deleted malware is shown in the **Deleted** tab of the **Malware Removal** page.



The feature invokes protections to prevent false positives:

- We do not auto-delete any macOS files, based off the root certificate.
- We do not auto-delete protected system resource files.
- We do not auto-delete any Carbon Black files.
- We do not auto-delete regular document files that do not contain macOS-executable macros.
- We do a final check directly before the auto-delete is scheduled to see if the reputation of the hash has changed from KNOWN_MALWARE or if the hash of the file has changed to one that is not KNOWN_MALWARE; if so, the auto-delete is cancelled.

Fixed in this release

Efficacy enhancements and bug fixes

Issue ID	Description
DSEN-2902	This release includes an efficacy enhancement to the certificate whitelisting process. Please review this security bulletin for more detailed information. **This improvement requires customer action:** You must reconfigure all certificate whitelists by adding common name strings for the items currently whitelisted by ORG strings. Please refer to the following Knowledge Base articles for more information: • Cb Defense: How to Identify Whitelisted Certs That Should be Updated for the 3.3 Mac Sensor • Cb Defense: Does the Update to Certificate Whitelisting for the 3.3 Mac Sensor Affect Currently Conf... • Cb Defense: How to Update Certificate Whitelist for 3.3 Sensor on Mac
DSEN-1980	This release adds support for the reporting of MODIFY_SENSOR TTP, which increases visibility into sensor disablement and tamper attempts.
DSEN-4372	This release fixes an issue where terminate action reports were not showing on the Investigate page for binaries that started before the sensor was installed, although they were successfully terminated. The bug only affected binaries.
DSEN-4526	This release resolves an issue where manual deletion of files through the Admin file delete feature via the console would fail when the endpoint was behind a proxy.
DSEN-4665	This release includes a fix to ensure malicious installers (PKG) and disk images (DMG) are always blocked regardless of type of file open.

Performance and stability

Issue ID	Description
DSEN-643	This release improves expedited reputation requests to effectively parallelize requests for multiple new files dropped and executed on the

	endpoint at the same time, a common developer use-case. The improvement reduces perceived delays executing such files.
DSEN-3983	This release improves macOS PKG validation.
DSEN-3832	This release fixes CB Defense installer image mount issues in case of multiple CB Defense DMGs being mounted simultaneously.
DSEN-4393	This release resolves a potential SQL injection vulnerability by upgrading to embedded libsqlite to version 3.26.

Other

Issue ID	Description
DSEN-4495	This release includes an improvement that updates the cloud.pem sensor file to the latest version that is available during sensor upgrades. This out-of-date file caused an issue with some macOS sensors, which were unable to check-in after a backend certificate change.
DSEN-4233	This release includes an improvement where the MAC addresses of all macOS devices are recorded in the **macAddress** column of the CSV export file that is available for download on the **Endpoints** page.

Known issues and caveats

Description
Although Carbon Black officially dropped support for macOS versions 10.6 - 10.9 in the 3.1 release, 3.1 and 3.2 sensors would still install and operate on 10.8 - 10.9 (although not officially supported). In this release, we dropped this unofficial capability altogether, and the 3.3 sensor will no longer install on macOS versions 10.8 - 10.9. The last sensor version for 10.6-10.9 is 1.2.4 (EOL). The range of macOS versions covered is as follows: **3.x sensor: macOS 10.10 - 10.14.3 (official support)** **1.x sensor (EOL): 10.6 - 10.12** The following behavior is expected when pushing a 3.3 sensor upgrade (cloud, attended, and unattended) to 1.x sensors that are running on an unsupported OS: - Devices running 10.6-10.9 will not upgrade.

There is an infrequent known issue where the Malware Removal UI inaccurately reports the actions that were or were not taken. This issue will be resolved in an upcoming backend release.

Issue ID	Description
DSEN-2735	Device name in sensor management is case sensitive.
DSEN-2700	Rare issue where repmgr sporadically crashes on shutdown, typically when the network/cloud is unreachable.
DSEN-2543	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: --downgrade=1 --skip-kext-approval-check=1
DSEN-3740	When the device is removed from an AD domain, the sensor is still reflected as within that domain in 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	Cloud uninstall of the sensor takes a long time due to a change in the backend.
DSEN-3669	Old canary files, specifically with variable or random files names, are not always properly cleaned up by the sensor, which can cause ransomware false positives.
DSEN-4194	When performing a fresh attended install of the 3.3 sensor on macOS 10.14, an error message appears in the UI although the installation does proceed successfully. This can be caused by a slow driver cache on slow machines.
DSEN-4373	Parent information is missing in the console (parent pid -1, empty parent hash) for processes that started before the sensor was installed or while the sensor is in bypass mode and still running.