Cb Defense Mac Sensor 3.1

Cb Predictive Security Cloud®

Release Notes
June 2018

General Notes

These Cb Defense Sensor version 3.1 release notes are for the Mac operating system only.

Important Note

This release introduces a new code signing certificate. The 3.1 sensor will require KEXT approval to run upon a fresh sensor installation as well as an upgrade. If the devices are not provisioned with the approval, the sensor enters bypass mode. Carbon Black recommends using an MDM solution to push the approval. This is also mentioned in the caveats section below. Links to KB articles to further assist with this matter are included as well.

Release Checksums

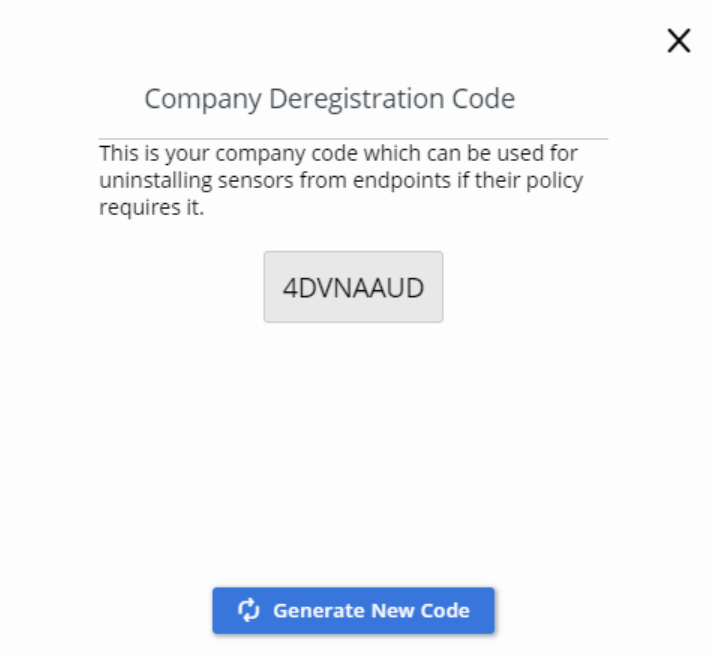
3.1.1.64 DMG SHA256 Checksum	501ee9a33647f3c9594ee796ab307bc2d05bb485dd460deccfe3b2bb1a241dfa
3.1.1.64 PKG SHA256 Checksum	bddee883ad84e0623b1e3158c067ee5d45bd902d3f5f5f5b7ac6f6cd8b8a703e

New Features

This section lists features introduced in the 3.1 version of Cb Defense Sensor. For a more thorough description of the new features in this release, see the Cb Defense User Guide.

Password Protected Uninstall

The 3.1 Cb Defense sensor provides admins additional control and protection of their endpoints by letting them require a code to uninstall sensors. Admins can now enable a policy setting that protects the action of uninstalling an endpoint by requiring a unique, randomly-generated code.



After this policy setting is enabled, admins can uninstall a group of sensors by using a company deregistration code, or uninstall sensors on a per-device basis by using an individual device uninstall code.

Note: To set the password protected uninstall feature, the checkbox must be selected, unselected, and selected again on the Policy page through the Cb Defense Management Console. This is a known issue, which is documented in the caveats below. This issue is slated to be fixed in the next macOS CbD sensor release.

Unattended Bypass Control

The unattended bypass control feature allows a user to enable and disable sensor bypass mode on the command line. This switch requires the uninstall code as a security measure. Admins and support users can troubleshoot the sensor and diagnose and collect logs more easily. Users can also recover from potentially critical conditions on the endpoint.

Carbon Black.

Issues Resolved in 3.1

List of issues resolved **since 3.0.2** release:

ID	Description
	Current effective sensor policy is more accurately reflected on the **Sensor Management** page.
DSEN-2597	Improved handling of “Invokes command interpreter” and “Invokes file-less script” blocking and isolation rules when applied to scripts to reduce false positives, when a rule should apply to the script interpreter only.
DSEN-2130	Ransomware: Upgraded Ransomware engine with improved detection accuracy and lower false positives.
DSEN-2034	Ransomware: Fix for stale hidden canary files that were not cleaned up by the sensor in some cases.
DSEN-2227	Reverse shell detection: false positive reduction improvements.
	Performance: faster reputation processing and reduced delay on execute for script files.
DSEN-2443 DSEN-2444 EA-12297	Code signing detection: Improved signature verification for universal binaries with tampered header and certificates revoked by Apple.
DSEN-1728	Sensor tamper protection improvements protecting repmgr service.
DSEN-1805 DSEN-1928	Minor miscellaneous security efficacy improvements

DSEN-2179	Fix for sensor datastore corruption that could lead to high CPU usage by repmgr service for an extended period.
DSEN-1930	Fix occasional sensor UI crash during sensor upgrade due to race with UI agent restart.
DSEN-2093	Upgraded internal libraries to include latest security patches and bugfixes
	cbdefense_install_unattended.sh script for unattended installation is now versioned. Added ***-v*** option to print out version number. Please always use the tool version matching the sensor release (extracted from the same DMG image). The script now checks for KEXT approval status before unattended install / upgrade, and aborts the installation if Cb Defense KEXT is not pre-approved. Administrator can override the check by using the ***--skip-kext-approval-check*** option, and proceed with install/upgrade to approve KEXT after the 3.1 sensor deploy.

Known Issues and Caveats

The following section lists known issues in this version of Cb Defense sensor.

Description
This release introduces a new code signing certificate. The 3.1 sensor will require KEXT approval to run upon a fresh sensor installation as well as an upgrade. If the devices are not provisioned with the approval, the sensor enters bypass mode. Carbon Black recommends using an MDM solution to push the approval. The KB articles below have been created or updated with additional information

Carbon Black.

New KEXT bundle ID: com.carbonblack.defense.kext

New Common name: ***Carbon Black, Inc.***

New Team ID: ***7AGZNQ2S2T***

To review the impact on installs and upgrades, as well as some additional tips, please review the following KB articles:

UPDATED: Cb Defense: How to approve Mac Sensor 3.0 KEXT for Install/Upgrade
https://community.carbonblack.com/docs/DOC-12365
UPDATED: Cb Defense: Why does KEXT approval show Scargo Inc as Developer for new cert?
https://community.carbonblack.com/docs/DOC-11891
NEW: Cb Defense: How to approve Mac Sensor 3.1 KEXT for Install/Upgrade
https://community.carbonblack.com/docs/DOC-14333
NEW: Cb Defense: Why do I need to re-approve KEXT after upgrading to Mac Sensor 3.1?
https://community.carbonblack.com/docs/DOC-14334
UPDATED: Cb Defense: Mac Sensor installs with status "Sensor Bypass Admin Action"
https://community.carbonblack.com/docs/DOC-11997

- As part of this release, the naming of the KEXT bundleID has changed from com.confer.sensor.kext to com.carbonblack.defense.kext
- In addition to this, the install location name has changed from /System/Library/Extensions/ConferSensor.kext to /System/Library/Extensions/CbDefenseSensor.kext

We are dropping official support for macOS versions 10.6 - 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 - 10.13 (official support)

1.X sensor (EOL): 10.6 - 10.12

The following behavior is expected when pushing 3.0 sensor upgrade (cloud, attended, and unattended) to 1.X sensors that are running on an unsupported OS:

- Devices running 10.6-10.7 will not upgrade. Devices running 10.8-10.9 will upgrade to 3.0 but will be running an unsupported sensor version for that OS.

Sensor installations on macOS 10.13, High Sierra, require initial KEXT approval of the product kernel extension by administrative policy or end user. This new requirement enforced by Apple applies to all third-party products that have a driver component.

Cb Defense recommends that you preconfigure High Sierra devices with Cb Defense pre-approved drivers by using MDM policy, netboot, or pre-configured images. This approach simplifies sensor deployment, especially in unattended mode.

If Cb Defense drivers are not pre-approved before sensor installation, the behavior is as follows:

- Unattended installation: installation finalizes and returns success, but logs a warning to installation logs. Because CB Defense drivers cannot load, sensor enters Bypass state and reports this state to the cloud. After KEXT is approved (either by an end-user or an administrator with MDM policy), the sensor recovers within one hour and enters the full protection state.

- Attended installation is handled similarly to unattended, with two differences: (1) sensor installation displays a dialog message that requests the end user to approve the KEXT using system preferences; (2) installer stalls for up 10 minutes, giving a user a chance to approve the KEXT.

To identify devices with sensors not supporting currently loaded OS, go to the **Sensor Management** page, change Status filter to **All**, and type the following search query:

sensorStates:UNSUPPORTED_OS

Use the following search query to help identify devices with sensors that do support the new OS but with sensor KEXT not approved:

sensorStates:DRIVER_INIT_ERROR

See *Apple Technical Note TN2459* for more details and recommendations for enterprise.

Certificate Whitelisting feature introduced in 3.0 does not fully support PKG installers. Although the rule does apply to trusted, signed and verified PKG files, it currently does not extend to files that are embedded in the trusted signed PKG installers.

New installer code format: To fresh-install 3.0 sensors, use the 3.0-supported company installation and individual device installation codes. This might require a configuration update to software deployment tools.

To set the password protected uninstall feature, the checkbox must be selected, unselected, and selected again on the Policy page in the Cb Defense Management Console.
Changed command-line interface for sensor unattended uninstallation to require a confirmation switch. The change might require an update of remote management tools. The new unattended procedure can be invoked via: */Applications/Confer.app/uninstall -y*
Certain environments can cause the sensor UI application to take focus of the local UI even when sensor UI is disabled. This is rare.
If you are using script *cbdefense_install_unattended.sh* for **unattended sensor installation or upgrade**, update your software deployment environment to use the script for 3.0 sensor DMG (extracted from */Volumes/CbDefense-3.0.X.X/docs/cbdefense_install_unattended.sh*). The script for 1.X installers is not compatible with 3.0 installer PKG. Please always use *cbdefense_install_unattended.sh* tool matching the sensor release.
Due to enhanced installer protections and a new reputation engine, downgrades from 3.1 and 3.0 to 1.2 are not supported out-of-the-box. Contact Support if this downgrade is required. Uninstall and install is an alternative to a downgrade path; however, this process results in a new device ID and loss of linkage to the original device data. Please note that the downgrade from 3.1 to 3.0 are also subject to KEXT approval due to the certificate change.
Live Response feature on macOS does not currently include the memory dump command.

Policy: ***Use Windows Security Center***: setting has no affect on Mac.

Policy: ***Delay Execute for Cloud Scan***: setting has no effect on Mac devices. Mac sensor implicitly enables delay execute for cloud scan, based on the configured policy rules. The delay is disabled when no prevention rules are present or when the only policy rules are for "Application" targets:

- "At path"
- "Company Blacklist"

Otherwise, the delay is implicitly enabled to facilitate rules that rely on the cloud reputations and make policy enforcement decisions at pre-execution time.