8.5.0 MAC AGENT RELEASE NOTES

Build: 8.5.0.72
Date: 17 March, 2021

Introduction

This document provides change information regarding VMware Carbon Black CB Protection 8.5.0 Mac agents and instructions for installation.

Note: VMware Carbon Black App Control Server v8.5.0 included rebranding. Previous versions were referred to as Cb Protection. The server product is now Carbon Black App Control and references in the software and documentation reflect that change.
This Mac Agent is still branded as Cb Protection and will be rebranded App Control in a future release.

Installation

As of the 8.1.4 server release, the Mac Agent no longer comes bundled with the App Server, nor does it require manual (command line) steps to add it to the server. You can upgrade Mac Agents without having to upgrade their App Control Server. Please visit the latest *App Control User Guide* for more information.

For information regarding what Mac operating systems are supported in this release, please review the CB Response sensors & CB Protection agents document on the Carbon Black User Exchange.

Purpose of This Release

The v8.5.0 Mac Agent provides improved performance, security, and new branding for the user interface.

For more detailed information, please review the specific sections carefully:

- New Features and Product Enhancements
- Corrective Content
- Known Issues and Limitations

Carbon Black.

New Features and Product Enhancements

Product security is our top priority. In this release, we have included several new enhancements to ensure that our product is prepared to keep you and your endpoints secure. These changes include:

- Added Mac Agent support for macOS Big Sur.

General Notes Regarding Installing, Upgrading, or uninstalling a Mac Agent

- Mac Agents support only Intel-based Mac hardware. Apple Silicon based hardware is not supported.
- After uninstalling a Mac Agent, we recommend rebooting the machine.
- The Mac Agent daemon 'b9daemon' (display name) must have full disk access.

Important Information Regarding Big Sur

The following information is pertinent to agent machines running MacOS 11.x Big Sur:

- MacOS 11.x (Big Sur) is not supported on any App Control Mac Agent prior to v8.5.0.
- After installing or upgrading a Mac Agent, manual approval of KEXT is required on MacOS 11.x Big Sur. After manual approval of KEXT, reboot the machine.
- After installing or upgrading a Mac Agent on a machine running MacOS 11.x Big Sur, a reboot of the machine is required. See: https://support.apple.com/en-in/HT211860
  NOTE: Reboot is not required for MacOS versions lower than MacOS 11.x Big Sur.
- If you are using the console to upgrade or install Mac Agents running MacOS 11.x Big Sur, then your admin must add post-installation MDM policies to reboot the MacOS 11.x Big Sur machines after installation or upgrade.
- Upgrade workflow for Mac Agent 7.3.x and any macOS prior to 11.x Big Sur

If…	Then…
Mac Agent 7.3.x is installed and MacOS is lower than 11.x (Big Sur)	We recommend that you upgrade the Mac Agent to 8.x first, and then upgrade the macOS to 11.x (Big Sur).
The user upgrades the MacOS to 11.x Big Sur before upgrading the Mac Agent to 8.x	The Mac Agent will not work. In this scenario, the user must: 1. Uninstall the 7.3.x Mac Agent. 2. Reboot the machine. 3. Install Mac Agent 8.x.

Corrective Content

This section lists defects fixed in the 8.5.0 Mac Agent.

Item #	Description
EP- 11901	Fixed an issue where some text in approval popups was unreadable if the OS is configured for dark mode.
EP- 12065	Fixed an issue where product copyright information was incorrect.
EP-12561	Fixed an issue discovered during internal testing where there was a rare chance of a deadlock scenario resulting in agent unresponsiveness.

Known Issues and Limitations

The following table lists the known issues and limitations present in the 8.5.0 Mac Agent.

Item #	Description
EP-805	On Mac and Linux systems, you cannot disable or replace the CB Protection logo in Notifiers. If you disable the logo, you may observe computer management events indicating "Computer failed to receive Notifier Logo: Source[…/GenericLogo.gif]". These should be disregarded.
EP-3392	Starting the Mac Protection agent through CLI using **/Applications/Bit9/Tools/b9cli -startup** fails to start the b9Notifier.
EP-4044	To avoid unwanted blocks relating to system updates generated from a Mac upgrade, we recommend using the Updater *Mac System Updates*. Please see the "Approving by Updater" topic in the *CB Protection User Guide* for more information.
EP-5820	Thunderbolt devices do not display Vendor Names.
EP-5821	Software RAID 0/1 device control status is always "Unapproved" and cannot be manipulated through device control.
EP-5960	Removable devices previously attached on the Mac endpoint may produce a "Never Seen" CLI message when you run the **/Applications/Bit9/Tools/b9cli --devices** command if that removable device approval state has been changed while it was unattached. Reinitializing the agent updates the device information appropriately.
EP-5965	While a removable device is banned (with writes and executes blocked), the user can still run *touch* on existing files and modify the modification timestamp.
EP-5967	A "new device found" message displays anytime a removable device is attached to an agent-managed Mac computer, even if it is a known, removable device.

Item #	Description
EP-5983	Removable devices attached on the Mac endpoint may produce a “Pending” approval state when running the CLI command, **/Applications/Bit9/Tools/b9cli --devices**, when the device approval state has changed after previously being “Approved”. We recommend you use the *Device Details* page of the CB Protection console to obtain this information.
EP-5986	When you run the CLI command: **/Applications/Bit9/Tools/b9cli --devices**, the results may produce the volume name of the previously attached removable device instead of the currently attached device. Reinitializing the agent updates the device information appropriately.
EP-5992	Symbolic links can be created on a banned removable device (with writes and executions blocked) and executed when pointing to binaries stored off of the removable device.
EP-6055	The CB Protection agent for Mac does not capture extended file attributes.
EP-6078	On Mac, an interoperability issue exists with certain versions of Trend Micro’s endpoint security products. You must run Trend Micro’s TMSM version 1.5 SP4 (or higher) to avoid this issue.
EP-6079	For Mac and Linux agents, the default uninstall behavior is now to remove all CB Protection agent data. Previous releases required an additional parameter (“-d”) for this data to be removed. In this release, you must use the (“-d”) parameter to *prevent* data removal.
EP-6080	On Mac systems, when chroot is used, the patterns for script processors may need to be changed to patterns that will be appropriately matched in the re-rooted environment. For example, in place of “/bin/bash”, you may want to use “*/bin/bash”. Contact Carbon Black Support for additional assistance.

Item #	Description
EP-6081	When CB Response is integrated with CB Protection, no information from CB Response sensors (including their presence or absence) is reported to the CB Protection server from Mac and Linux systems. Integration with CB Response works only on systems running a CB Protection Windows agent.
EP-6082	When you run a Custom Rule to test an execution block on a macOS system, the agent may report that the process for the blocked execution is xpcproxy. This is a normal condition based on the implementation of the Mac operating system. When creating a rule that applies to applications invoked from the typical launching mechanisms of Finder and/or launched on Mac, it is best to also include */usr/lib/dyld* as a potential parent for the application.
EP-7320	The Mac Agent erroneously lists the hard drive along with removable devices in Macs running macOS 10.13.6 (or later). You cannot alter the state of the hard drive, nor is there any impact to agent functionality.
EP-11562	Logging out of the console does not stop the notifier from running.
EP- 12140	Some notification text requires more clarity.
EP- 12180	MD5 and sha1 hashes for new, interesting files do not display on the server.
NA	Beginning with 10.13.4 High Sierra, Apple's *Secure Kext Loading* feature now extends to MDM deployments. As such, Carbon Black kernel extensions will need to be approved ahead of MDM deployment using our Team and Bundle IDs. Please see https://community.carbonblack.com/docs/DOC-13277 for more information.
NA	When approving the CB Protection Kext (Kernel Extension) on 10.14.5 Mojave a warning will appear noting "One or more system extensions that you have approved will be incompatible with a future version of macOS. Please contact "Carbon Black, Inc." for support". This warning can be ignored.

Contacting VMware Carbon Black Support

Please view our Customer Support Guide on the User Exchange for more information about Technical Support:

https://community.carbonblack.com/t5/Support-Zone/Guide-to-Carbon-Black-Customer-Support/ta-p/34324

For your convenience, support for Carbon Black CB Protection is available through several channels:

Technical Support Contact Options
Web: User eXchange
E-mail: support@carbonblack.com
Phone: 877.248.9098

Reporting Problems

When you call or email technical support, please provide the following information to the support representative:

Required Information	Description
Contact	Your name, company name, telephone number, and e-mail address
Product version	Product name (for example, CB Protection Server or Agent) and version number
Hardware configuration	Hardware configuration of the server or endpoint having the issue (processor, memory, and RAM)
Problem	Action causing the problem, error message returned, and event log output (as appropriate)
Problem severity	Critical, Major, Minor, Request