CB PROTECTION

Release Notes: Mac Agent 7.3.0

May 2019

Introduction

This document provides information for users installing Cb Protection v7.3.0.36 Mac agents.

This v7.3.0 Mac agent no longer requires manual installation, however, you will need to have CB Protection Server 8.1.4 or above. Please visit the CB Protection Server 8.1.4 User Guide for more information about installing and upgrading agents under this new process.

Once these files are installed, they may be used to deploy agents on Mac systems.

Purpose of This Release

The CB Protection Mac Agent v7.3.0 (7.3.0.36) release addresses a critical bug causing intermittent system freezes to occur on agent managed Macs running 10.14 Mojave.

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

Corrective Content

This release provides the following corrective content changes:

- CB Protection agent no longer allows for per-agent CLI passwords by default. [EP-7432]
- Updated copyright information with b9cli output. [EP-6695]
- Mac Protection has been updated to support Xcode10. [EP-6133]
- Addressed bug with an authorization that could trigger a reboot shortly after login. [EP-7895]
- Addressed bug with memory consumption used in determining User ID process information. [EP-7455]
- Addressed bug with disposing of the Notifier Prompt icon. [EP-5141]
- Addressed bug with displaying Notifier Prompts on primary monitor displays when a fullscreen application is in use. [EP-7862]
- Addressed bug where Mac Protection agent, running on 10.13.6 (or later), incorrectly reported the Mac hard drive as a device registered on the Mac endpoint. [EP-6732]
- Addressed bug with attempting to create volume pointers with invalid device memory. [EP-7138]
- Addressed bug with reporting file opens using Expert rules. [EP-7905]

Known Issues and Limitations

This section lists known issues and limitations of this Mac agent release. See also the *Known Issues and Limitation*s section in the separate Release Notes for your CB Protection Server version for issues that might be relevant to this Mac agent release.

- The Mac Protection icon is incorrectly displayed as an aqua blue dot from the Toolbar and Activity Monitor when running Dark Mode on 10.14 Mojave. [EP-6651]
- 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-805]
- Starting the Mac Protection agent through CLI using **/Applications/Bit9/Tools/b9cli -startup** fails to start the b9notifier. [EP-3392]
- To avoid unwanted blocks relating to system updates generated from a Mac upgrade it is recommended to use the Updater *Mac System Updates*. Please see the “Approving by Updater” topic in the *CB Protection User Guide* for more information. [EP-4044]

- Thunderbolt devices are not displaying Vendor Names. [EP-5820]

- Software RAID 0/1 device control status is always “Unapproved” and cannot be manipulated through device control. [EP-5821]

- 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 will update the device information appropriately. [EP-5960]

- 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-5965]

- A “new device found” message will appear anytime a removable device is attached to an agent-managed Mac computer. [EP-5967]

- Removable devices attached on the Mac endpoint may produce a “Pending” approval state when running the **/Applications/Bit9/Tools/b9cli --devices** command when the device approval state has changed after previously being “Approved”. This information should be obtained through the *Device Details* page of the CB Protection console. [EP-5983]

- When you run the **/Applications/Bit9/Tools/b9cli --devices** command, the results may produce the volume name of the previously attached removable device instead of the currently attached device. Reinitializing the agent will update the device information appropriately. [EP-5986]

- 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-5992]

- The CB Protection agent for Mac does not capture extended file attributes. [EP-6055]

- 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-6078]

- 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. The same parameter now *prevents* data removal. [EP-6079]

- 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. [EP-6080]

- 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-6081]

- 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-6082]

- 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.

- 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 Carbon Black Support

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

- **Web:** User eXchange
- **Email:** support@carbonblack.com
- **Phone:** 877.248.9098
- **Fax:** 617.393.7499

Reporting Problems

When you call or e-mail technical support, please provide the following information to the support representative:

- **Contact:** Your name, company name, telephone number, and email address
- **Product version**: Product name (CB Protection server and agent version)
- **Hardware configuration:** Hardware configuration of the CB Protection 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, the error message returned, and event log output (as appropriate)
- **Problem severity:** Critical, serious, minor, or enhancement request