CB PROTECTION

Release Notes: 7.3.4 Mac Agent

September 2020

Introduction

This document provides change information regarding CB Protection v7.3.4.102 Mac agents and instructions for installation.

Installation

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

IMPORTANT NOTE: Automatic upgrades do not work with the CB Protection v7.3.4.102 Mac agent. This is a known issue. We've provided suggestions below to automate the installation process using an MDM. However, you can also upgrade the Mac agent using the CB Protection User Guide.

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 CB Protection v7.3.4 (7.3.4.102) Mac Agent is considered a maintenance release with a focus on improved security, user interface fixes, and reliability. Changes include:

- Added ability to password protect config list files.
- Added ability for Mac Agent to accept encrypted config list files.
- Fixed CB Protections's appearance in Dark Mode.
- Fixed Cmd-A issue; it is no longer a Mac Agent shortcut.
- Fixed several issues to improve product reliability.

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

New Features and Product Enhancements

Product security is our top priority for CB Protection. 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 ability for the customer to create password-protected Config List files. After creating the password on the server, it is passed to the agent where it is used to decrypt the Config List file.

  This provides an additional layer of security to your network. You get to determine the password used to encrypt and decrypt your Config List files.

- Added ability for the Mac agent to accept encrypted Config List files.

  This provides an additional layer of added security to your network. The Config List remains encrypted between the server and local agent, thus preventing unauthorized users from surreptitiously gaining access to what rules are in effect. No unencrypted copies of the configuration list are stored on disk.

Automating CB Protection Upgrades Using an MDM Tool

We understand the administrative overhead the inability to install the mac agent via the console, so to help you streamline this process we've included a guide below on how you can automate the install of the agent across your environment(s) using Smart Groups.

We specifically used JAMF to automate this process, but we are aware there are different tools that can be used. (Note: This is just one of the many workflows that could be potentially used to install the agent)

If you are doing an install for the first time, there is no need to follow these instructions, but to follow the normal installation instructions using our Host Package Installer.

To properly upgrade the CB Protection agent, you will need to use the 'Bit9MacInstall.bsx.pkg'.

In our method to upgrade we used a set of three different MDM polices. It is possible to use a single policy to accomplish this task, but using multiple policies serves as an error check "safeguard".

- In order for the following MDM policies to work you will need to be able to detect the version of Protection and the status of Tamper Protect on scoped agent machines. We did this using two extension attributes that runs a b9cli –status and grep the data needed.

Our first MDM policy will be used to disable Tamper Protect on the agent machines to be upgraded. This policy will use the data we grepped from the b9cli –status to determine the state of the agent. If Tamper Protect is enabled, this policy will disable it. (Note: In order to disable this, you will need to use the global password for your agents to do this.)

Our Second MDM policy will be set to upgrade Protection on ANY computer that has Tamper Protect disabled and is on an agent version < 7.3.4.102. This policy will use the data we grepped from the b9cli –status to determine both pieces of information we need. This policy will also run the 'Bit9MacInstall.bsx.pkg' which will actually perform the agent upgrade. (Note: When this script is completed there is no need to restart the agent machine being upgraded)

Our Third MDM policy will be set to restore Tamper Protection on upgraded agent machines. This policy will be set to ANY computer that has Tamper Protect disabled and is on the agent version 7.3.4.102. This policy once again will use the information grepped from b9cli –status.

Using this policy workflow, you should be able successfully upgrade your mac endpoints with this new version of CB Protection

Carbon Black.

Corrective Content

This section lists defects fixed in this release, CB Protection 7.3.4.102 Mac Agent.

Item #	Description
EP-6050	Fixed issue where if the “Cmd-A” shortcut was used in a CB Protection notification window, it selected **Allow**. This was problematic because Cmd-A in a MAC is normally the command to “select all”. Now, “Cmd-A” is no longer recognized as a shortcut for **Allow** in the notification window.
EP-6651	Fixed a Dark Mode issue where the CB Protection icon incorrectly displayed as a pale, blue dot from the Toolbar and Activity Monitor. This problem was specific to Dark Mode on 10.14 Mojave macOS. Now, the CB Protection icon displays correctly in macOS 10.14 Mojave Dark Mode.
EP-7477	Fixed an issue where a crash sometimes occurred when the agent Notifier window closed. Now, closure of the agent Notifier window does not crash the Mac Agent.
EP-8653	Fixed the following user interface issues: • Replaced all old Bit9 logos with Carbon Black Protection logos. • Corrected issue where Notifier dialog buttons were unreadable in macOS Dark Mode. Now, the user interface displays correct logos and dialog buttons in Dark Mode display correctly
EP-9296	Fixed issue where MAC agents intermittently did not receive prompts for new, unapproved files. The problem could only be resolved by rebooting the endpoint. Now, MAC agents consistently receive prompts for new, unapproved files.
EP-9392	Fixed a macOS Catalina issue where if a user approved a file, the Notifier prompt erroneously reappeared the next time the file was run despite the fact that the file was already approved. Now, if a macOS Catalina user approves a file, it remains approved.

Item #	Description
EP-9433	Fixed issue where Notifier displayed the patch version in an incorrect format. Now, the Notifier correctly displays the version as: *7.3.4.xx*
EP-9522	Fixed issue where the customer was not able to approve devices connected to Mac endpoints if the device media name was five (5) characters long. Now, users can approve media if the name is five (5) characters long.
EP-9603	Fixed issue where if an internal drive had “Media” as a device name suffix, that drive would erroneously be changed to a USB type drive. Now, an IOMedia type drive continues to be defined as IOMedia regardless of the device name suffix.
EP-10184	Fixed issue where the database encryption key exported during diagnostics was not in a format compatible with Windows. Now, an encrypted database can be opened on a Windows system with the proper encryption key.
EP-10986	Fixed issue where some agents reported “kernel panic” during initialization.

Known Issues and Limitations

The following table lists the known issues and limitations present in the CB Protection 7.3.4.102 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.
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.

Carbon Black.

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/community/resources/support/pages/about

For your convenience, support for 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