CB PROTECTION

Release Notes: Mac Agent 7.2.3 Patch 11

October 2018

Introduction

This document provides instructions for adding the latest Cb Protection Mac agent to either a Cb Protection Server v8.1.0, v8.0.0 or a Bit9 Platform Server v7.2.3. Cb Protection Servers v8.1.0 and v8.0.0 do not currently include an agent that can be installed on macOS endpoints, so completion of these instructions is the only way to add a Mac agent. Although Bit9 Platform Server v7.2.3 does include a Mac agent, these instructions allow you to upgrade to the latest version.

System Requirements

The instructions in this document assume that you have either Bit9 Server v7.2.3 or Cb Protection Server v8.0.0 (or later) installed.

Purpose of This Release

The Cb Protection Mac Agent v7.2.3.3985 (Patch 11) release provides support for Apple's 10.14 Mojave macOS.

Installation Instructions

To complete deployment of the new Mac agents, do the following:

- **Install the Mac System Updates updater:** Install the Mac System Updates updater provided with this release, or if you have automatic cloud updates enabled, check to see that the Mac System Updates updater is at Version 9 or later.
- **Add the new agent files to the server:** Add the new files for agent installation to the Cb Protection Server or Bit9 Server, as described in this document.
- **Upgrade or install the agent:** Follow the instructions for upgrading or installing the macOS agent.
- **Allow the kernel extension:** If you are not using MDM and are currently running High Sierra 10.13 (or later), complete the procedures for allowing the "Bit9, Inc." kernel either during (preferable) or after agent installation.
- **Upgrade the OS:** After you install or upgrade the agent, if you are upgrading the macOS to High Sierra (or later), disable the agent, upgrade the macOS, and then return the agent to its normal policy.

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

Included Files

The following files are included with this release:

- Agent installation files, which you will copy to the Cb Protection Server:
  - **Bit9Agent.pkg**: The agent installation setup package.
  - **Bit9MacInstall.bsx**: The agent installation program.
- Additional files to copy to the server to allow approval and deployment of the agent files, and to enable automatic upgrades:
  - **MacGeneratedFilesToApprove.sql**: A SQL script to approve the Mac agent files on the Cb Protection Server.
  - **MacAgent-Upgrade.xml**: Adding the content of this file to upgrade.xml will allow the agents to work with our automatic upgrade capability.
  - **MacSystemUpdate.b9u**: Version 9 of the Mac System Updates updater; for use if you have not been automatically updated to this version via the cloud.
- Documentation files:
  - **cbprotection-release-notes-for-Mac-agent.pdf:** This is the release notes document for the release (i.e., the document you are reading).

Confirm That the Mac System Updates Updater Is At Version 9 or Later

The Cb Protection updater named Mac System Updates allows updates to the OS to be approved. This updater should be at least at version 9 before you install the new agent. If you have enabled cloud updates to your Cb Protection Updaters, you might already have version 9. You can check for this on the Updaters page.

To manually update the Mac Systems Updates updater:

1. Copy the updater file **MacSystemUpdate.b9u** to a location accessible from the Cb Protection server.
2. If you are running a v8.0.0 server (or later), you must make a change on the Support.php page to show the Add Updater button:
   a. After logging into the console, enter **https://***<serveraddress>***/Support.php** in the browser address field and select the **Advanced Configuration** tab.
   b. In the Software rules section, check the box in the **Show Import Buttons** field and then click the **Update** button at the bottom of the page.
3. Choose **Rules > Software Rules** on the console menu and select the **Updaters** tab.
4. Click the **Add Updater** button.
5. In the Add Updater dialog, specify the **MacSystemUpdate.b9u** updater file, enter the password **bit9** and click the **Save** button. This imports the new version (version 9) of the Mac System Updates updater to the server. The updated version will automatically be pushed to Mac agents associated with the server.

Adding the Mac Agent Files on the Cb Protection Server

Next, you add the Mac agent files to the Cb Protection Server so that agents can be deployed in the standard way from the console.

To add the Mac agent files to the Cb Protection Server:

1. Make sure you are running **Bit9 Server version 7.2.3** or **Cb Protection Server version 8.0.0 (or later)**. Bit9 Server v7.2.3 already includes the Mac agent as part of that release, but adding the files described here allows you to upgrade those agents. Cb Protection Server v8.1.0 and v8.0.0 do not ship with a Mac agent and therefore require these files if you want to protect macOS systems.
2. If there is an agent on the server, disable the agent's tamper protection before proceeding.
3. You must enable generation of Mac installers if this feature has been disabled on your server (the default in 8.0.0 and later versions):
    a. Log in to the Cb Protection Console as an Administrator, and navigate your browser to **http://***<servername.domainname>***/shepherd_config.php**.
    b. On the Defined Properties menu, choose **GenerateMacInstaller** and enter **true** in the Property value field.
    c. Click the **Change** button.
4. Stop the Cb Protection or Bit9 Platform Server by running the following command:
    - net stop ParityServer
5. The file **MacGeneratedFilesToApprove.sql** is included with this distribution. Run this SQL script from within SQL Management Studio to approve all Mac agent content.
6. Copy the .pkg and .bsx files provided with this agent release to the **hostpkg** folder on the Cb Protection Server. If you used the default installation directory, this folder is **c:\Program Files (x86)\Bit9\Parity Server\hostpkg** (for 64-bit server OS)
7. Update **upgrade.xml** to allow existing agents to be upgraded to this version. If you used the default installation directory, upgrade.xml is located in the following folder: **c:\Program Files (x86)\Bit9\Parity Server\upgrade** (for 64-bit server OS)
    - Open **upgrade.xml** for editing.
    - Open the **MacAgent-Upgrade.xml** file provided with this distribution. There are separate sections for 7.2.x servers and 8.0.0 servers. In the section that matches your server version, copy the contents of that section only, beginning with **<!-- Mac Upgrade -- >**.
    - If the upgrade.xml already has a **<!-- Mac Upgrade -- >** section, replace that section with the version you copied from MacAgent-Upgrade.xml. Otherwise, paste the new section you copied into upgrade.xml, just above </upgradelist>.
8. Restart the Parity Server service by running the following command:
    - net start ParityServer
9. If you disabled tamper protection for an agent on the server, make sure agent tamper protection is re-enabled.

Upgrading an Existing Agent

After you update agent files on the server, you have these options for upgrading existing agents:

- If the agent is in a policy with automatic upgrades enabled, the server will schedule the update – no action is required on your part for this step.
- You can select computers on the Computers page in the console and force agent upgrades using commands on the Action menu.
- You can use the manual, command-line-based upgrade.

Important: Changes have been made to the Cb Protection agent installer to accommodate **Secure Kernel Extension Loading (SKEL)** introduced in macOS High Sierra (10.13). For all of the methods above, if you are not using MDM and are currently on any version of High Sierra (or later), see the section Allowing the agent kernel extension in High Sierra for additional, mandatory steps to allow the Bit9, Inc. kernel extension.

Remediating Kernel Panics on Sierra and El Capitan

If you have a previous Cb Protection agent installed and you updated to the 2018-001 security updates for Sierra and El Capitan before upgrading to this Cb Protection agent, kernel panics will result. To be able boot the systems and upgrade the agents on these systems, you must do the following on each system:

1. Shut down the device entirely.
2. Boot the box back up in Recovery Mode (Command + R).
3. Open the Disk Utility, and mount the Macintosh HD (or whatever the drive name is). This requires a password.
4. Close the Disk Utility, and in the top bar select Utilities > Terminal.
5. Run the following commands:
    a. **cd /Volumes/Macintosh HD/Library/Extensions**
    b. **rm -rf b9kernel.kext**
6. Reboot the device, which should now allow you to login again.
7. Uninstall the agent.

Additional information regarding booting the device in safe mode can be found on the Apple support site using the following link https://support.apple.com/en-us/HT201262.

Manual Agent Upgrades

To manually upgrade a 7.2.0 or later Mac agent:

1. Log in to the Cb Protection (or Bit9) console.
2. Either disable Tamper Protection for the agent or move it to a Disabled mode policy.
3. In the console, choose **Rules > Policies** and click on the download agent software link at the top of the Policies page.
4. Download the upgrade installer for Mac agents, which is **Bit9MacInstall.bsx**. You can do this by using a URL, UNC path, or any other standard means of getting to the file. Note that this installer is not listed on the Downloads page in the console.

   To use a URL, you can choose **Rules > Policies** in the console, click on the Download link at the top of the page, and edit the URL for the download page as follows:

   https://<serveraddress>**/hostpkg/pkg.php?pkg=Bit9MacInstall.bsx**
5. Open a Terminal window and change directory to the location where the installer was downloaded (by default, the user-specific Download directory).
   cd ~/Downloads
6. Enter the following command to install the agent:
   sudo bash Bit9MacInstall.bsx
7. If you are not using MDM and are currently on any version of High Sierra, see the section Allowing the agent kernel extension in High Sierra for additional, mandatory steps to allow the Bit9, Inc. kernel extension.

Installing an Agent on Systems with no Existing Agent

The following instructions apply to systems that do not have a Cb Protection or Bit9 Agent installed.

Important: Changes have been made to the Cb Protection agent installer to accommodate **Secure Kernel Extension Loading (SKEL)** introduced in macOS High Sierra (10.13). These Secure Kernel Extension Loading changes can cause a block message to appear during agent installation. If you are not using MDM and are currently on any version of High Sierra, see either of the following for additional mandatory steps to allow the Cb Protection Agent to run:

- **Allow the extension on the Security & Privacy dialog** – This option is described in Allowing the agent kernel extension in High Sierra and can be done immediately when prompted during agent installation, or later.
- **Whitelist the extension via Team ID** – This option is described in Team ID whitelisting option for the kernel extension. If you choose this option, it should be done before running the agent installation procedure.

For systems currently running earlier versions of macOS or if you are running MDM, you will not need to take either of these steps. In addition, if an agent was previously installed and then uninstalled, the kernel extension sometimes will retain approval and load without prompting. In these cases, you will not see SKEL warnings and do not need to use either of the options for allowing the extension.

Agent Installation

You begin agent installation by downloading the agent installation package for your operating system and policy. If you use AD-based policy assignment, you may use the Mac installer for any policy that allows automatic policy assignment. The same agent installer can be used on multiple endpoints, and can be distributed to endpoints via SSH or distribution mechanisms like Casper. See “Downloading Agent Installers” in the Cb Protection user guide for more details.

To install a new agent:

1. Log in to the Cb Protection (or Bit9) console.
2. Either disable Tamper Protection for the agent or move it to a Disabled mode policy.
3. In the console, choose **Rules > Policies** and click on the download agent software link at the top of the Policies page.
4. Download the appropriate installer DMG file. Installers for Mac are named by policy: <*policyname*>**-mac.dmg**
5. In a Terminal window, change directory to the location where the installer was downloaded (by default, the user-specific Download directory).
   cd ~/Downloads
6. Double-click on the agent installation file you downloaded to initiate a standard package installation dialog.
7. Unless the kernel extension is allowed because of a previous agent installation or use of the Team ID procedure, dialogs will report that a system extension signed by “Bit9, Inc.” was blocked. When these appear, navigate to **System Preferences > Security & Privacy**, click **Allow** for “Bit9, Inc.”, and restart the agent. See Allowing the agent kernel extension in High Sierra for more details.

   Important: If the kernel extension is not allowed to load, installation continues, and the agent connects to the server and initializes, but it will not enforce rules.
8. Respond to any other prompts, and when the dialog indicates the installation was successful, click **Close**. If you allowed the “Bit9, Inc.” kernel extension, the agent begins operating correctly immediately.
9. For enhanced security, the Cb Protection agent self-protects its application directory. If you run anti-virus software, exclude the following directories from AV scanning to avoid performance problems:
   - **/Applications/Bit9/Daemon/b9daemon** – the Cb Protection Agent process
   - **/Applications/Bit9** – the Cb Protection program directory
   - **/Library/Application Support/com.bit9.agent** – the Cb Protection data directory

- **/Library/Extensions/b9kernel.kext** – the Cb Protection driver location for OS X 10.9 (Mavericks) and later -or- /System/Library/Extensions/b9kernel.kext – the Cb Protection driver location for OS X versions prior to 10.9

10. The Mac firewall may detect the agent as a new application and block access to the network. Instruct users to permanently allow incoming connections to b9daemon.

Allowing the Agent Kernel Extension in High Sierra (or later macOS)

Note: If you are using a version of macOS prior to 10.13 the steps described in this section are not necessary.

MacOS High Sierra introduced changes in the way system extensions are handled. If you are installing or upgrading the Cb Protection Agent on any version of 10.13 (or later) additional steps are needed to approve the “Bit9, Inc.” system extension, which is required for proper operation of the agent. This is true for manual agent installations and upgrades as well as those initiated from the Cb Protection Console.

For non-MDM installations on High Sierra (or later), while you are running the Cb Protection Agent installer, macOS will report that a system extension signed by “Bit9, Inc.” was blocked. This will happen even if the extension is already whitelisted on the system. When this message appears, go to **System Preferences > Security & Privacy** and click the **Allow** button for “Bit9, Inc.”.

Important: If you do not allow the kernel extension, agent installation continues, and the upgraded agent will connect to the server, but it will not enforce rules until you allow the extension to load. On the Cb Protection console, this agent will show a status of Unprotected, Reboot Required. If this is the case, see Allowing the extension after installation is complete.

Allowing the Kernel Extension after Installation Is Complete

It is possible that you delay or are unable to allow the kernel extension immediately after agent installation or upgrade. For example, you might automatically upgrade unattended endpoints.

To allow the Bit9, Inc. kernel extension after agent installation:

1. Navigate to **System Preferences > Security & Privacy** on the endpoint and click the **Allow** button for “Bit9, Inc.”.
2. Do one of the following to restart the agent:
   - reboot the agent system, or
   - manually stop and start the agent (you must log in to b9cli with a password first):

     ./b9cli –password
     ./b9cli –tamperprotect 0
     ./b9cli –shutdown
     sudo ./b9cli –startup

     (**Note:** *Must be run as root or using sudo)*

Checking Agent Status

Especially given the kernel extension issues in High Sierra, you might want to carefully monitor the status of new or upgraded agents. You can passively monitor Mac agent status by using the Platform filter on the Computers page (**Assets > Computers**) to show all Mac agents. A blue dot means the agent is connected and healthy. You can also check the Upgrade Status and Policy Status columns to determine whether the agent is unprotected.

Health checks may also report the status of agents. They run periodically as a scheduled job on the server, but you can also prioritize a health check for a specific computer so it runs as soon as possible. You do this from the Advanced menu on the Computer Details page. Results of an agent health check would be one of the following:

- Cb Protection Agent is healthy. Options[$param1$].
- Cb Protection Agent failed a health check. ErrorsFound[$param2$] Options[$param1$]
- Cb Protection Agent detected a problem: $param1$. $param2$

If you determine from looking at the Computers page or receiving a health check that a Mac agent might not be fully protected, consider going through the steps in Allowing the extension after installation is complete. Within a few minutes the console should show the agent with a blue status and Policy Status as protected.

Team ID Whitelisting Option for The Kernel Extension

If you prefer, you can whitelist the Team ID for the “Bit9, Inc.” kernel extension before installing the Cb Protection agent rather than allowing the extension to load during installation. This option requires root access and booting into Recovery Mode.

To use Team ID whitelisting to allow the kernel extension:

1. Boot into Recovery Mode by either holding CMD+R at boot time or typing the following into a Terminal and rebooting: sudo nvram "recovery-boot-mode=unused"
2. Once in Recovery Mode, open a Terminal and type the following: spctl kext-consent add 7AGZNQ2S2T
3. Reboot, and install the agent normally after downloading the agent installation package from the server.

Upgrading to Mojave with an Agent Installed

Important: For systems running existing agents prior to 7.2.3 Patch 11, do not upgrade to Mojave 10.14 before upgrading to the Patch 11 agent. Previous agents are not compatible with 10.14 macOS.

Updating from one major OS version to another with an agent in place requires disabling the agent during the upgrade. If you are upgrading to Mojave, take the following steps on each system:

1. Complete all the agent upgrades.
2. Place the agent in Disabled mode.
3. Upgrade the operating system to Mojave
4. Once the macOS update is completed, move the agent back into to its previous policy. It will begin to reinitialize its files.

Additional Information about Agents

Additional information about agent installation and maintenance is available in Chapter 4, “Managing Computers,” of the user guide for your version of the Bit9 or Cb Protection Server. These can be downloaded through the User eXchange or accessed via online help in the console:

- For Cb Protection v8.1.0, see https://community.carbonblack.com/docs/DOC-16661.
- For Cb Protection v8.0.0, see https://community.carbonblack.com/docs/DOC-6378.
- For Bit9 Security Platform v7.2.3, see https://community.carbonblack.com/docs/DOC-4484.

Corrective Content

This release provides the following corrective content changes:

- Updated Mac Protection agent to allow for installation on 10.14 Mojave macOS. [EP-5786]

Known Issues and Limitations

This section lists known issues and limitations of this macOS 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 v7.2.3 MacOS agent release.

- Users running the Mac Protection agent on macOS 10.13.6 (or later) should be aware that the agent reports the Mac hard drive (or virtual partition) as a device registered on the Mac endpoint, however this Mac hard drive device cannot be banned/approved (i.e. *Device Control Settings* will not apply to Mac hard drive device). [EP-6732]

- 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 macOS. [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 MacOS 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 MacOS 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 MacOS computer. [EP-5967]

- Removable devices attached on the MacOS 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 MacOS, 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 macOS operating system. When creating a rule that applies to applications invoked from the typical launching mechanisms of Finder and/or launched on macOS, it is best to also include /usr/lib/dyld as a potential parent for the application. [EP-6082]

- Beginning with MacOS 10.13.4, 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.

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, error message returned, and event log output (as appropriate)
- **Problem severity:** Critical, serious, minor, or enhancement request