8.6.2 WINDOWS AGENT RELEASE NOTES

Build: 8.6.2.8

Date: August 26, 2021

The VMware Carbon Black App Control v8.6.2 Windows Agent Release Notes document provides information for users upgrading from previous versions as well as for users new to Carbon Black App Control.

This document is divided into the following sections:

- Installation

  This section provides information regarding the installation of the Carbon Black App Control v8.6.2 Windows Agent.

  NOTE: See new Installation Note before uninstalling agent.

- Purpose of this release

  This section describes the purpose of the Carbon Black App Control v8.6.2 Windows Agent release.

- New Features and Product Enhancements

  This section describes the new features and product improvements added to the Carbon Black App Control v8.6.2 Windows Agent.

- Corrective Content

  This section describes issues resolved by the Carbon Black App Control v8.6.2 Windows Agent.

- Known Issues and Limitations

  This section describes the known issues or anomalies in the Carbon Black App Control v8.6.2 Windows Agent that you should be aware of.

- Contacting Carbon Black Support

  This section describes ways to contact Carbon Black Technical Support, and the information to prepare that will help troubleshoot a problem.

- Appendix 1: New Features, Enhancements, and Corrective Content in Previous 8.x Windows Agent Releases

  For those upgrading to a v8.x-series Windows Agent release for the first time, this section provides a quick reference to other changes introduced in previous 8.x Windows Agent releases.

This document is a supplement to the main Carbon Black App Control documentation.

Installation

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

Note: This Windows Agent is compatible with App Control Server version 8.1.4 and subsequent releases.

For information regarding what Windows operating systems are supported in this release, please review the Carbon Black EDR sensors & Carbon Black App Control agents document on the Carbon Black User Exchange.

Purpose of this release

The Carbon Black App Control v8.6.2 Windows Agent is a maintenance release to address two important issues. Please see Corrective Content for details.

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

- Corrective Content
- Known Issues and Limitations

Corrective Content

This section lists defects fixed in the Carbon Black App Control 8.6.2 Windows Agent.

Item #	Description
EP-12850	Fixed an issue that could block the starting of office applications after Office is updated using ClickToRun.
EP-13363	Fixed an issue that blocked the agent from running on Server 2003.

Known Issues and Limitations

The following table lists the known issues and limitations present in the Carbon Black App Control 8.6.2 Windows Agent.

Item #	Description
EP-1201	On Windows 2003 x64, you may see a health check reporting improper classifications immediately after installation. This should go away after roughly fifteen minutes.
EP-1682	Carbon Black App Control does not support in-container enforcement. Users can use the Microsoft Edge Virtualization feature, but Carbon Black App Control will not enforce rules within the container. It will, however, enforce rules on anything that breaks out of the sandbox.
EP-2393	The appearance in the console of block and report events related to the Ransomware rapid config may be delayed by a minute or more.
EP-5483	The agent currently tracks all the extracted content from the Windows 10 WIM image in the temp directory. A rule to ignore these writes is not yet functioning properly.
EP-5498	In some cases, the agent will report an empty installer for a given file. The file will still be correctly approved or not, as expected on the endpoint. Only reporting of the source installer is failing, not enforcement of relevant rules.
EP-6104	Cleanmgr.exe is a windows utility process that runs occasionally and will copy files to the "temp" folder in order to run analysis on them. These files are only copies of other files already on the machine and cleanmgr.exe never executes them.

Item #	Description
EP-6106	An installation of a new Carbon Black App Control Agent on the latest version of Windows 10 can result in a health check error due to a miscalculation of how many events the agent should send to the Carbon Black App Control server. This problem disappears after a reboot.
EP-6107	After upgrading agents on Windows XP systems, it is possible to see signature error events stating that the installer download failed. The upgrade should be successful and there should not be any impact on the upgrade process.
EP-6197	Occasionally the agent will complain about metadata not being properly populated and trigger an Error. The Error implies a mismatch in expectation but is not expected to break functionality of the agent and can be ignored.
EP-6982	Carbon Black App Control does not support NTFS reparse points as exclusion paths and they should not be used with kernelFileOpExclusions configuration rules. Reparse points include such objects like symbolic links, directory junction points and volume mount points.
EP-8505	On Windows XP, If EDR and APPC are installed, uninstalling Appc will get stuck. This is XP specific issue. As workaround uninstall EDR first [reboot machine] and uninstall App control.
EP-11127	There is a known issue where the Microsoft OneDrive application binaries are marked dirty every time they are executed. To determine if a file is possibly a OneDrive file, the Windows agent checks if OneDrive is enabled on the system and currently checks for \OneDrive\ in the path. If so, the agent does not analyze the file during traversal and if executed, analyzes the file every time because OneDrive files can change without our knowledge. The path check can also match the OneDrive binaries themselves, causing unneeded re-analysis.

Item #	Description
EP-10542	When uninstalling the agent, a Carbon Black App Control Agent dialog displays informing the user that certain applications must be closed before continuing the installation. This informational message is caused by a known msiexec defect: https://support.microsoft.com/en-ph/help/2745579/same-file-or-service-name-causes-incorrect-fileinuse-dialog **IMPORTANT NOTE:** This could occur during a removal of the agent using "add/remove programs" or during an upgrade of the agent if you are using 3rd party software or a manual upgrade using msiexec. Customers that perform agent upgrades from within the Carbon Black App Control Admin console are not affected. When uninstalling the agent or performing a manual upgrade, or upgrade using 3rd party software, you can suppress this dialog with the additional msiexec command line argument "/qb-". This will disable modal dialog during manual uninstalls and upgrades. The example below shows how to manually uninstall the Carbon Black App Control agent with the /qb- argument: `msiexec /x {9F2D4E59-0528-4B22-B664-A6B0B8B482EE} /qb-` This issue is not new to the Windows agent and possibly affected customers on earlier releases. A long term fix will be implemented in a future release.

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 App Control 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, Carbon Black App Control 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

Appendix 1:
New Features, Enhancements, and Corrective Content in Previous 8.x Windows Agent Releases

For those upgrading to a v8.x-series Windows Agent release for the first time, this section provides a quick reference to other changes introduced in previous 8.x Windows Agent releases.

NOTE: As of 8.5.0, all product references are to App Control.

- **App Control Windows Agent v8.6.0**
  - New Features and Product Enhancements
  - Corrective Content
- **App Control Windows Agent v8.5.0**
  - New Features and Product Enhancements
  - Corrective Content
- **CB Protection v8.1.10 Windows Agent**
  - Product Enhancements
  - Corrective Content
- **CB Protection v8.1.8 Windows Agent**
  - Product Enhancements
  - Corrective Content
- **CB Protection v8.1.6 Windows Agent**
  - New Features and Product Enhancements
  - Corrective Content
- **CB Protection v8.1.4 Windows Agent**
  - Corrective Content
- **CB Protection v8.1.0 Patch 2 Windows Agent**
  - Corrective Content
- **CB Protection v8.1.0 GA Windows Agent**
  - Corrective Content

App Control Windows Agent 8.6.0

New Features and Product Enhancements

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

- Added a config property to mitigate an issue where performance on network shares was negatively impacted by App Control's DFS share detection code.
- Made a change to reduce excessive network traffic by sending non-critical, system information to the server less often. Default value is now every 12 hours.
- Improved EDR Healthcheck events by making the text more EDR-specific.
- Improved log formatting by adding a “date” prefix to each entry. Previously, the only prefix was the time.
- Added a new, configurable property that delays rule checking until rules have been expanded for a new user.

Product Security Enhancements:

- Improved security by using the fileid when handling file deletion requests.
- Improved security be ensuring that the Config List encryption key is stored in such a way that it is available even if the DB and backup DB becomes corrupt.

Corrective Content

This section lists defects fixed in the Carbon Black App Control 8.6.0.162 Windows Agent.

Item #	Description
EP-8360	Fixed an issue that could cause performance issues on large Citrix environments.
EP-8383	Fixed an issue that led to unintended App Control Tamper Protection blocks at the time of computer startup.
EP-10548	Fixed an issue where the event description for the Event Subtype: "File deletion processed (file not found)" did not display the file hash.
EP-11234	Fixed an issue where old branding names remained in the registry. Upon upgrade, the old registry items are updated.
EP-11237	Fixed an issue where custom logos did not display on Windows 7 or Windows XP machines.

Item #	Description
EP-11238	Fixed an issue that could potentially cause the machine to crash upon driver unload.
EP-11494	Fixed an issue where a process approval rule could cause file rules to stop working by short circuiting internal rule optimizations.
EP-11910	Fixed an issue that could, under rare circumstances, cause the machine to crash.
EP-11920	Fixed an issue where event text for blocked and reported reads required additional information.
EP-11950	Fixed an issue where the publisher name hash was computed incorrectly due to trailing spaces.
EP-12024	Fixed an issue where visibility mode caused sharing violations which prevented software upgrades.

App Control Windows Agent v8.5.0

Installation

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

Note: This Windows Agent is compatible with App Control Server version 8.1.4 and subsequent releases.

For information regarding what Windows operating systems are supported in this release, please review the Carbon Black EDR sensors & Carbon Black App Control agents document on the Carbon Black User Exchange.

IMPORTANT NOTE:
There is a known Microsoft issue where you may see a "File in use" dialog.

This could occur during a removal of the agent using "add/remove programs" or during an upgrade of the agent if you are using 3rd party software or a manual upgrade using msiexec.

Customers that perform agent upgrades from within the Carbon Black App Control Admin console are not affected.

When uninstalling the agent or performing a manual upgrade, or upgrade using 3rd party software, you can suppress this dialog with the additional msiexec command line argument "/qb-". This will disable modal dialog during manual uninstall/update
The example below shows how to manually uninstall the Carbon Black App Control agent with the /qb- argument:

```
msiexec /x  {9F2D4E59-0528-4B22-B664-A6B0B8B482EE} /qb-
```

This issue is not new to the v8.5.0 Windows agent and possibly affected customers on earlier releases. A long term fix will be implemented in a future release.

This is documented below as known issue EP-10542.

New Features and Product Enhancements

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

Branding Changes:

- Rebranded the agent and documentation to Carbon Black App Control.
  The following changes are also reflected in the User Interface and documentation:
    - CB Predictive Security Cloud (PSC) is now Carbon Black Cloud
    - CB Response is now Carbon Black EDR
    - CB Collective Cloud Defense is now Carbon Black File Reputation

Product Security Enhancements:

- Updated the hashing algorithm used for global CLI passwords for agents version 8.5.0 and above. The MD5 hash has been replaced with the SHA-256 hash.
- Replaced a 3rd party OpenSSL library with the Windows OpenSSL library

Corrective Content

This section lists defects fixed in the Carbon Black App Control 8.5.0.103 Windows Agent.

Item #	Description
EP-10295	Fixed an issue where TimedOverride.exe could not be executed by multiple non-admin users . TimedOverride.exe now works with multiple non-admin users. Each user gets their own log file in <profile_dir>\AppData\Local\VMware\TimedOverride
EP-10320	Fixed an issue where the agent package installer would back up the entire hostpkg directory, every time the agent was upgraded. The host package installer no longer backs up the entire hostpkg directory.
EP-10478	Fixed an issue that could cause unnecessary reboots during an upgrade. **NOTE**: This problem exists in prior agents and customers upgrading from older versions of the Windows Agent could still run into issues. This fix addresses the issue moving forward, starting with Windows Agent 8.5.0 and above.
EP-10613	Fixed an issue where the server asked the agent to remove a Certificate Rule, but this rule did not exist on the Agent. The misleading error message no longer occurs.
EP-11152	Fixed an issue where Parity.exe could crash on due to information being delivered in an unexpected format.
EP-11201	Fixed a rare, intermittent issue where some servers experienced a blue screen after upgrading the agent.
EP-11241	Fixed an issue where the agent could cause a BSOD after upgrading to 8.1.8 on some platforms. This was due to a timing issue where the Parity driver could call crypto functions from CNG.SYS before the driver was initialized. Now, the Parity driver waits for the CNG driver to create a device before calling any crypto functions.
EP-11275	Fixed an issue where interesting files, larger than 512MB caused an “Execution Block (still analyzing)” event for the file.

CB Protection v8.1.10 Windows Agent

Installation

As of the 8.1.4 server release, the Windows 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 Windows Agents without having to upgrade the CB Protection Server. Please see the latest *CB Protection User Guide* for more information.

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

IMPORTANT NOTE:
There is a known Microsoft issue where you may see a "File in use" dialog.

This could occur during a removal of the agent using "add/remove programs" or during an upgrade of the agent if you are using 3rd party software or a manual upgrade using msiexec.

Customers that perform agent upgrades from within the CB Protection Admin console are not affected.

When uninstalling the agent or performing a manual upgrade, or upgrade using 3rd party software, you can suppress this dialog with the additional msiexec command line argument "/qb-". This will disable modal dialog during manual uninstall/update
The example below shows how to manually uninstall the CB Protection agent with the /qb- argument:

```
msiexec /x  {9F2D4E59-0528-4B22-B664-A6B0B8B482EE} /qb-
```

This issue is not new to the 8.1.10 Windows agent and possibly affected customers on earlier releases. A long term fix will be implemented in a future release.

This is documented below as known issue EP-10542.

Purpose of this release

The 8.1.10.88 Windows Agent is considered a maintenance release with a focus on corrective content.

Product Enhancement

- Replaced OpenSSL with the native Windows encryption libraries.

Corrective Content

This section lists defects fixed in CB Protection 8.1.10.88 Windows Agent.

Item #	Description
EP-11275	Fixed an issue that limits the size of the file which can be analyzed due to constrains of 32 bit processor architecture.

Item #	Description
EP-11273	Fixed an issue where user specific rules were not being enabled until after the user had logged in.
EP-11241	Fixed an issue where system crashes were caused by the agent calling functions from the CNG.SYS before the driver was initialized.

CB Protection v8.1.8 Windows Agent

Installation

As of the 8.1.4 server release, the Windows 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 Windows Agents without having to upgrade the CB Protection Server. Please see the latest *CB Protection User Guide* for more information.

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

IMPORTANT NOTE:
There is a known Microsoft issue where you may see a "File in use" dialog.

This could occur during a removal of the agent using "add/remove programs" or during an upgrade of the agent if you are using 3rd party software or a manual upgrade using msiexec.

Customers that perform agent upgrades from within the CB Protection Admin console are not affected.

When uninstalling the agent or performing a manual upgrade, or upgrade using 3rd party software, you can suppress this dialog with the additional msiexec command line argument "/qb-". This will disable modal dialog during manual uninstall/update
The example below shows how to manually uninstall the CB Protection agent with the /qb- argument:

```
msiexec /x  {9F2D4E59-0528-4B22-B664-A6B0B8B482EE} /qb-
```

This issue is not new to the 8.1.8 Windows agent and possibly affected customers on earlier releases. A long term fix will be implemented in a future release.

This is documented below as known issue EP-10542.

Purpose of this release

The 8.1.8 Windows Agent is considered a maintenance release with a focus on corrective content, security and third-party library updates.

Product Enhancements

These changes include:

- When a user authenticates a dascli session and executes 'dascli as part of the status.
- Added a default agent configuration setting to ignore three extensions associated with MS-SQL files (**mdf, ldf, ndf**) if the agent detects MS-SQL is installed. Prior to this change some customers with agents deployed on their MS-SQL servers would observe contention problems on SQL data files during system startup due to agent cache checks. This would cause the database to go into "Recovery Pending" state.

Third-party Library Cleanup

- We updated the minizip library to use wincrypt API (FIPS certified).
  Parity uses the minizip library to extract rules and create diagnostics.

Security Enhancements

- Fixed an issue where Yara sometimes failed to analyze a file, especially if the file was large. Now, the system falls back to internal file analysis if Yara analysis fails.

Corrective Content

This section lists defects fixed in the CB Protection 8.1.8 Windows Agent.

Item #	Description
EP-5537	Fixed an issue where some certificates were not being marked as expired. (Trusted Publishers and certificate rules were not affected by this).
EP-7887	Fixed an issue where occasionally after upgrading to 8.1.0, the agent would not repair its registry keys so the error "Cb Protection Agent detected a problem: Cb Protection Agent was unable to load cached rules from the registry. Enforcement from boot will be limited. Options[00000003] TotalFailures[1] FailureId[930]" will persist with low enforcement risk to endpoints.
EP-7981	Fixed an issue in Parity.sys where a page fault could cause the operating system to crash.
EP-9051	Fixed an issue with agent upgrades being pushed from the console when the agent is disabled and the agent would fail causing the upgrade to abort.
EP-9186	Fixed an issue where a user rule to block reads from removable media did not work in some instances.
EP-9521	Fixed an issue that was causing the operating system to crash due to failed memory allocation.
EP-9535 EP-9620	In Windows agent versions prior to 8.1.8, the script processors opening the associated scripts with write privileges would be treated as a script execute and therefore blocked as unapproved. Now, script processors will not be blocked as “unapproved” when opening associated scripts with write privileges.
EP-9536	Fixed an issue where suspicious file events were being sent to the server when MSI files had appended data, even if the MSI file was not signed. Now, we send the event, "Msi file has data appended after the signature.", only if the MSI file was signed.

Item #	Description
EP-9786	Fixed a bug where MSP files were omitted from the cache consistency check that applies the fuzzy hashing algorithm to MSI/MSP files. In previous versions, this could lead to unexpected blocks on MSP files that had been previously approved.
EP-9858	Fixed an issue in the logic which handles expanding wild card path names, the agent was failing to correctly identify certain paths for well-known windows images, and was incorrectly classifying them as missing.
EP-9889	Fixed a race condition in the CB Protection agent that can cause the operating system to crash.
EP-9972	Fixed an issue with mmap write rules not blocking correctly.
EP-9976	Fixed an issue where the file driver could prevent other processes, such as SCCM, from accessing files opened by the parity service which was creating a sharing violation.
EP-10162	Fixed an issue where Kernel Process Exclusions were not working correctly under certain conditions.
EP-10222	Fixed a performance issue when processing MSI files that contain files greater than 500MB.
EP-10230	Fixed a performance issue with Chrome version 80 and higher. The performance problem would occur after opening the browser after a new install or upgrade.

CB Protection v8.1.6 Windows Agent

New Features and Product Enhancements

CB Protection 8.1.6 Windows Agent provides the following improvements and enhancements:

Purpose of This Release

The 8.1.6 Windows Agent is considered a maintenance release with a focus on corrective content, security and Windows 10 Update Performance.

Our research into Windows 10 update performance showed that we had a long-time regression that went back to our 8.0 release. In prior versions of 8.x, the agent would unnecessarily analyze files repeatedly during file opens and file cleanups; file cleanup is an OS command that tells us that all of the handles to the file have been closed (e.g. every program/thread/process that could be using the file is done with it). In 8.1.6, customers should notice an improvement in performance during Windows Updates. We've also added some additional logging and instrumentation to further enhance the collection and tracking of agent performance metrics so that we can collect better data to further improve performance of the Windows agent in future releases.

The following minor changes have been made:

Added a TimedOverride.bt9 file that now logs when TimedOverride.exe is launched. This new log file is found in the **Bit9\Parity Agent\logs** folder.

Added a new agent configuration property, "skip_session_enumeration_in_scm". When this setting is enabled in a Citrix/Multi-user environment, user enumeration will be disabled. This will lead to performance improvements but will break user-based policy determination and will slow the update time of logged-in users at the console. We expect this setting to be used only for very specific environments.

Removed the authentication requirement for the dascli ValidateCerts command

For more detailed information please review the "Corrective Content" and the "Known Issues and Limitations" sections carefully.

Product Security Enhancements

Product security is our top priority for CB Protection, and 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:

- Fixed an issue that could allow some files to be launched by msiexec even though they were not approved.
- Addressed a vulnerability where it was possible to remove CB Protection without disabling Tamper Protection.
- Fixed an issue where it was possible to execute unapproved .Net Core Console applications when those applications should have been blocked by custom rules

Corrective Content

This section lists the defects that were fixed in CB Protection 8.1.6 Windows Agent.

Corrective Content in CB Protection 8.1.6 Windows Agent (Build 212)	
Item #	**Description**
EP-8000	Fixed an issue during installation or upgrade of the agent that would cause the agent to BSOD when referencing a non-existing process.
EP-8194	Fixed an issue where Microsoft Teams Installer was not being recognized as an installer. This should also help with other installer files as the Yara rules have been updated to find setup.exe in some metadata fields and mark a file as an installer based off that. Customers will need to upgrade to the 8.1.6 server and perform a Cache Consistency Check using "Full Scan for New Files" to detect these installers.
EP-8396	Fixed an issue where the agent service wouldn't start due to libraries not being loaded in the correct order.
EP-8424	Fixed an issue with path entries that were formatted incorrectly. During upgrade to the 8.1.6 Windows agent, the paths will be corrected and you will see a corresponding event in the admin console.
EP-8431	Fixed an issue where Active Directory rules were not working correctly when the endpoint was not connected to the domain.
EP-8843	Fixed an issue with the agent that could cause the agent to be non-functional after a Major Windows Upgrade.
EP-8850	Fixed an issue where an agent could crash if an Agent Configuration property was missing the "=" statement.
EP-8904	Fixed an issue where the agent would hang during a certificate check.
EP-8958	Fixed a timing issue that was causing numerous 'Server Config List Error' events.
EP-9358	Fixed an issue where the agent could crash during a certificate check.

CB Protection v8.1.4 Windows Agent

Corrective Content

This section lists the defects that were fixed in CB Protection 8.1.4 Windows Agent.

Corrective Content in CB Protection 8.1.4 Windows Agent (Build 173)	
Item #	**Description**
EP-2768	Previously, tamper protection enforcement by the Windows agent was preventing Windows from cleaning up control sets in the registry after a restart. Symptoms of this problem were an accumulation of registry keys in HKLM\System that are no longer needed and many tamper protection block events in the console that indicate services.exe was blocked from deleting ControlSetXxx. The agent now allows the OS to delete old ControlSetXxx from registry without blocks from tamper protection and related tamper protection events.
EP-6990	Agents will now send an event when the agent completes a policy change. Previously, the agent would only generate an event when an Administrator moved an agent from one policy to another but not when the agent actually received and completed the policy change (unless the enforcement level also changed). The two new events associated with this change are "Policy change was scheduled for" and "Policy change was completed".
EP-7302	Enhancements were made to how the agent analyzes MSI files and what MSI files the agent finds interesting.
EP-8230	Fixed an issue where Service Control Messages were being sent synchronously, which could cause login delays and timeouts on terminal servers during user logins. The agent now defers expensive service control messages to be asynchronously updated.
EP-8230	Fixed an issue where Rule Expansion could take a long time and could cause agents to disconnect from the server.
EP-7629	Fixed an issue where the agent was reporting “Database errors discovered” during a clean install of the agent.
EP-8284	Fixed a bug where creating multiple script rules with the same extension could trigger multiple cache consistency checks, incorrectly approving files.
EP-7694	Fixed an issue with multiple dascli commands that could cause dascli to crash.

Corrective Content in CB Protection 8.1.4 Windows Agent (Build 173)	
Item #	**Description**
EP-8094	Fixed a defect involving reparse points where in some environments the agent would crash while trying to determine the file name.
EP-6885	Resolved an issue where a Windows API call was causing an exception when examining MSI's and could lead to the agent crashing.
EP-5507	Fixed an issue with buffer size that was causing performance issues during account lookup.
EP-6971	Fixed an issue that was preventing agent diagnostic files from being deleted from the agent machine after being uploaded to the CBP Server. Upon a successful upload of the agent's diagnostic files to the server, all of the agent's diagnostic files are now automatically deleted from the agent machine.

CB Protection v8.1.0 Patch 2 Windows Agent

Corrective Content

This section lists the defects that were fixed in CB Protection 8.1.0 Patch 2 Windows Agent.

Corrective Content in CB Protection 8.1.0 Patch 2 (Build 3546) – Windows Agent	
Item #	**Description**
EP-6200	Fixed the noisy assert in the agent process tracking that would complain about PID 4 not being enumerated.
EP-6144	Fixed the information caching issue where sometimes the agent would give the following error stating "isLocal mismatch Kernel[x] Usermode [y]".
EP-4988	Fixed an issue where a critical system process, for example ntoskrnl.exe, may be tagged by CB Protection Agent as Bit9:Terminated which results in blocks of any I/O the process performs before it is terminated. Because critical system processes cannot be terminated by the Agent, the issue persists until the system is rebooted or the tag is removed by using expert rule tagging actions.
EP-1543	To reduce the number of expanded rules, the system will wildcard per user rules (e.g. C:\Users*\Documents) instead of expanding the rule once per logged in user. If a user has changed their folder location, this release will always include an expansion for the changed location.
EP-3481	Fixed an issue where files could be silently blocked even after Allow was clicked when being prompted by the notifier.
EP-5280	Updated the OpenSSL version the agent uses to 1.0.2o
EP-6866	Fixed an issue where the agent would, under some circumstances, scan the computer for new scripts on every startup. Users may see a small positive performance impact.
EP-7067	Fixed an issue where it was possible the machine would hang upon reboot after upgrading the CB Protection agent.

CB Protection v8.1.0 GA Windows Agent

Corrective Content

This section lists the defects that were fixed in CB Protection 8.1.0 Windows Agent.

Corrective Content in CB Protection 8.1.0 (Build 3324) – Windows Agent	
Item #	**Description**
EP-3521	Fix for BSOD in VM layering environments due to pushing of Protection upgrade layer while keeping old registry data after agent upgrade.
EP-2751	Rolling logging of Agent Logs was not working correctly. Some logs would get lost and agent config properties such as max_rolling_trace_size_mb and max_rolled_trace_logs_to_keep would not be obeyed. Now rolling logging works correctly.
EP-3217	A problem was identified that could lead to system files installed by Windows Update to not be approved properly if updates were installed more than fifteen minutes apart from each other. This affects agents running 8.0.0 Patch 3 through 8.0.0 Patch 5 but is now addressed.
EP-2400	Under some circumstances, when removable drives are connected to a system running the agent during system restart, duplicate records of a file may have been created, triggering errors in the agent logs and error events on the server. This is corrected.
EP-1199	Event for timed override completion was missing. Added event notification for this and also fixed bug where timed override could cause the agent to stop sending events to the server until restart.