Cb Protection v8.0.0

Release Notes

Product Version 8.0.0.2621 (Patch 7)
7 May 2018

Carbon Black, Inc.
1100 Winter Street, Waltham, MA 02451 USA
Tel: 617.393.7400 Fax: 617.393.7499
E-mail: support@carbonblack.com
Web: http://www.carbonblack.com

Introduction

The *Cb Protection v8.0.0 Release Notes* document provides information for users upgrading from previous versions as well as for users new to Cb Protection. It consists of the following major sections:

- **Before you begin**: This section describes preparations you should make before beginning the installation process for Cb Protection Server.
- **New Features in this Release**: This section describes new features added in this patch release.
- **Cb Protection Platform 8.0.0 new and modified features**: For those upgrading to v8.0.0 for the first time, this section provides a quick reference to other changes introduced in previous 8.0.0 releases.
- **Agent Operating System Support Notes**: This section describes several special cases for agent operating system support in this release.
- **Corrective content:** This section describes issues resolved by this release as well as more general improvements in performance or behavior.
- **Known issues and limitations:** This section describes known issues or anomalies in this release of Cb Protection v8.0.0 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.

This document is a supplement to the main Cb Protection documentation.

Purpose of this Release

This release provides support for OneDrive Files On-Demand and adds a Rapid Config to Report or Block 'Doppleganging'. It also includes corrective content that resolves issues reported in previous releases.

About your Cb Protection Distribution

Your Cb Protection distribution includes the server installation program. Cb Protection Server custom-generates agent installation packages at your site for each protection policy you define, so no separate agent installer is needed in the original distribution.

Documentation

Your Cb Protection documentation set consists of online Help built into the Cb Protection Console and PDF files included with the product distribution and available on the Carbon Black User eXchange.

The standard documents include:

- **Installing the Cb Protection Server –** Provides instructions for installing and configuring the Cb Protection Server.

- **Using Cb Protection –** Describes Cb Protection operation, including step-by-step instructions for administration and configuration tasks. Management topics for computer systems, including **agent installation**, are also covered. The content of this document is available as online help in the Cb Protection Console and also as a PDF book file.
- **Cb Protection Events Integration Guide** – Describes the events that are generated, tracked, stored, and accessible through Cb Protection, and the ways you can access Cb Protection event data outside of the Cb Protection Console user interface.
- **Cb Protection API Documentation** – There are several sources of documentation for the Cb Protection API:
    - Instructions for configuring the Cb Protection API are included in Appendix B, "Cb Protection API," in *Using Cb Protection*.
    - Documentation for the Cb Protection REST API can be found at https://developer.carbonblack.com/reference/enterprise-protection.
    - Full documentation for the cross-product Carbon Black API is located at https://cbapi.readthedocs.io.
- **Other Documentation** – Additional documentation is available on the User eXchange for special topics, including integration with Unidesk, operating environment requirements, and supported operating systems for agents.

Before you Begin

This section describes preparations you should make before beginning the installation process for Cb Protection Server. These include actions you should take before installing the server, preparations you should make for configuring the server after installation, and general information you should know about the server and agent. It contains information that applies to upgrades and new installations.

System requirements

The document *Cb Protection Operating Environment Requirements v8.0.0* describes the hardware and software platform requirements for the Cb Protection Server and the SQL Server database that stores Cb Protection data. The document *Cb Protection Agent Supported Operating Systems v8.0.0* provides the current requirements for systems running the agent. Both are available to customers with login credentials on the Carbon Black User eXchange.

Both upgrade and new customers should be sure to meet the requirements before proceeding.

Cb Protection Server upgrades

This following section is for upgrades only. If you are not upgrading, see New Cb Protection Installations (page 6). For more detailed instructions, please refer to *Installing the Cb Protection Server*. It is available in the Carbon Black User eXchange.

Below is a table explaining the supported upgrade paths for Cb Protection servers

Upgrading from	Upgrading to
v5.1.2	⇨ v6.0.2 latest ⇨ v7.2.1 latest ⇨ v8.0.0
v6.0.0	⇨ v6.0.2 latest ⇨ v7.2.1 latest ⇨ v8.0.0
v6.0.1	⇨ v6.0.2 latest ⇨ v7.2.1 latest ⇨ v8.0.0
v6.0.2	⇨ v7.2.1 latest ⇨ v8.0.0
v7.0.0	⇨ v8.0.0
v7.0.1	⇨ v8.0.0
v7.2.0	⇨ v8.0.0
v7.2.1	⇨ v8.0.0
v7.2.2	⇨ v8.0.0
v7.2.3	⇨ v8.0.0
v8.0.0 previous versions	⇨ v8.0.0 current version

Support for the upgrade process

Cb Protection Server and agent update releases are covered under the Customer Cb Protection Maintenance Agreement. We recommend reviewing content on the User eXchange prior to performing the upgrade for the latest information that supplements the information contained in this document. Carbon Black Technical Support is available to assist with any issues that may develop during the upgrade process. Our Professional Services organization is available to assist with the upgrade process to ensure a smooth and efficient upgrade installation.

Rescanning of agents after server upgrade

When Cb Protection Server is upgraded from one major version to another (such as v7.2.0 to v8.0.0), ongoing enhancements to "interesting" file identification make it necessary to rescan the fixed drives on all Carbon Black-managed computers. These upgrades also require a new inventory of files in any trusted directories to determine whether there are previously ignored files that are now considered interesting. This process involves the same activity as agent initialization. It can cause considerable input/output activity and it can take minutes – or even hours – to complete depending upon the number of agents and the number of files. A gradual upgrade of agents is recommended to avoid an unacceptable impact on network and server performance. See "Enabling Automatic Agent Upgrades" in the *Using Cb Protection* guide for more details.

Before running the server upgrade

The following tasks should be done *before* you run the Cb Protection Server upgrade program:

- **Backup Cb Protection Server database:** Backup your Cb Protection Server database before you begin the upgrade process. You *must* have a recent backup available so that there is a recovery option in case of database update failure during server update.
- **Backup certificates separately:** In v8.0.0, Cb Protection Server's Certificates will be backed up in the Database. However, IIS certificates are not backed up automatically. Please do a separate backup of IIS certificates, and if upgrading from 7.0.0, all Cb Protection certificates, on a system other than the Cb Protection Server.
- **Disable distribution systems:** If you use third-party deployment mechanisms (e.g. SCCM), either: disable the distribution of the Cb Protection Agent using SCCM, and use Cb Protection Server for upgrading agents; or disable Cb Protection Server from upgrading agents, and use your third-party deployment mechanism to upgrade the agents.
- **Stop SQL background jobs:** Because the Cb Protection database is updated during a server upgrade, no other database jobs should be running. This includes background jobs on database maintenance and backups activity. Stop any of these jobs, and confirm that no one else is using the database before initiating the Cb Protection Server upgrade.
- **Disable Linux agent generation:** If you are generating installation packages for Linux agents on a pre-8.0.0 server, you should disable package generation before upgrading the server to v8.0.0 CD-1. Otherwise, the server will fail to generate agent installation packages *after* an upgrade. To disable Linux agent installer generation, log in to the console, go to **https://***<yourserver>***/shepherd_config.php**, and set the **GenerateRedhatInstaller** flag to **false** before upgrading.

Prepare for post-upgrade tasks

Be prepared to do the following tasks after you run the Cb Protection Server upgrade program.

- **Review external event settings:** If you use External Events, review the settings to ensure they are still enabled and correctly functioning.
- **Review updaters:** New Updaters have been added. Review the Updaters tab on the Software Rules page to make sure the correct updaters are enabled.
- **Update agent distribution points:** If you use third-party deployment mechanisms (e.g. SCCM), re-enable or re-create them using new agent packages from the upgraded Cb Protection Server. Use ParityHostAgent.msi to upgrade from a pre-v8.0.0 agent.
- **Review the new Cb Protection installations section:** Although it is for new installations, this section also includes information of possible interest to upgrade customers.
- **Enable System Health Indicators:** Cb Protection includes a System Health page, which reports on factors that affect the performance of your server, including the compliance of your environment with Operating Environment Requirements. Consider enabling this feature to keep your system healthy.

New Cb Protection installations

For more detailed instructions about preparations you must make, please refer to *Installing the Cb Protection Server*.

This section describes preparatory tasks and suggested post-installation tasks for new Cb Protection Server installations. Although targeted at new installations, it should be reviewed by new and upgrade customers.

Prepare for Cb Protection Server installation

- **Choose account for Cb Protection Server installation**: Use of a Domain Service Account is recommended for Cb Protection Server installation. If you plan to use Active Directory services or use an authenticated proxy to access the Internet, a Domain Account is required for Cb Protection Server Service. This account must have Local Administrator privileges on the Cb Protection Server.
  Note: Do not change the permissions level of the account with which you install Cb Protection after installation.
- **Prepare to enable Cb Protection Agent management access:** The Cb Protection Agent Management screen in the new installation dialog allows you to designate a user or group, or a password usable by anyone, to perform certain agent management activities assisted by Carbon Black Technical Support. Especially if you will have client computers that will never be connected to Cb Protection Server, it is best to set up a client access option before generating and distributing agent installation packages. If you are unable to configure access during installation, you can do it later on the Management Configuration page in the Cb Protection Console. See *Using Cb Protection* (or online help) for more details.

Prepare for post-installation tasks

- **Enable Cb Protection CLI management access:** If you did not enable Cb Protection Agent Management access during installation, go to the General tab of the System Configuration page in Cb Protection Console to enable it, preferably before deploying agents. See "Configuring Agent Management Privileges" in *Using Cb Protection* (or online help) for more details.
- **Confirm agent installation privileges:** The Cb Protection Agent installer must be run by a user with the appropriate administrative rights. On Windows, this can either be Local System or a user account that has administrative rights and a loadable user profile. On OS X and Linux, the user must be able to run as root (sudo is one of the techniques that may be used).
- **Consider agent rollout impact:** As soon as the Cb Protection Agent is installed, it connects with the server and begins file initialization to determine which files are interesting and should be reported to the server. Because initialization can involve an increased flow of data between the Cb Protection Server and its new client, be sure your agent rollout plans take your network capacity and number of files into account — simultaneous agent installation on all the computers on a large network is not recommended. Deploying agents in disabled mode will avoid this situation.
- **Review trusted updaters:** Ensure that that correct Review Trusted Updaters are enabled for your environment before you begin large-scale Cb Protection Agent deployment.
- **Review root certificates for trusted publishers:** Trusted Publishers are validated by Windows. For proper validation to occur, the correct, up-to-date root certificates must be installed for these publishers. You should ensure that Microsoft root certificate updates are included in your Windows Updates. If you plan to use in-house certificates, ensure that your in-house root certificates are installed on each endpoint on which you will install a Cb Protection Agent.
- **Test user-supplied certificates:** Cb Protection Server allows use of user-supplied certificates for Cb Protection Agent-Server communication. To validate this certificate, each agent system must have up-to-date root certificates. Test your new certificates before large-scale Cb Protection Agent deployment begins. See "Securing Agent-Server Communications" in *Using Cb Protection* or online Help for more details.
- **Review content of trusted directories for distribution systems:** If you use Windows Software Update Services (WSUS) or other software distribution mechanisms (e.g. SCCM or Altiris), pre-approving this content with a Trusted Directory before large-scale Cb Protection Agent deployment will ensure a more effective transition to High Enforcement Level.
- **Script Files:** It is most efficient to define your script rules before you install agents (or move them out of disabled mode) to avoid having to rescan the file system to look for those scripts**.** Java Tracking is an example. Support for tracking Java class and jar files is not enabled by default. If you plan to track Java applications, please choose **Rules->Software Rules** from the console menu and enable the rules for Java on the **Scripts** tab.
- **Exclude Cb Protection Agent from AV scanning:** Antivirus products, including Microsoft SCEP, should be configured to exclude Cb Protection Agent files from scanning. Please refer to the *Using Cb Protection* guide for detailed information about the files or folders to exclude for each platform.

- **Consider other agent interactions:** Certain other types of software may interact with the Cb Protection Agent – contact Carbon Black Support for more information on each of these cases:
    - Disk encryption software may interact with the Cb Protection Agent. In general, full disk or partition encryption should minimize the chances of problems. However, some encryption products are compatible with Cb Protection with other types of encryption (file or folder) enabled.
    - Ghosting or imaging systems with Cb Protection pre-installed requires additional steps on the master system. Please consult the "Managing Virtual Machines" chapter in the Using Cb Protection guide for more information.
- **SQL recovery model:** The simple recovery model is recommended. Use of the full recovery model may affect Cb Protection Server performance. If you intend to use the full recovery model, please contact Carbon Black Support for more information.
- **Enable System Health indicators:** Cb Protection v8.0.0 includes a System Health page, which reports on factors that affect the performance of your server, including the compliance of your environment with operating environment requirements. Consider enabling this feature to keep your system healthy.

New Features in this Release

The following features are new for this patch release. To see new features introduced in previous v8.0.0 versions, see New and Modified Features in v8.0.0 on page 10.

Rapid Config to Report or Block 'Doppleganging'

A Rapid Config was added to protect against exploits known as Doppelganging. Information about the Doppelganger exploit can be found here:
https://community.carbonblack.com/docs/DOC-11212

OneDrive Files On-Demand Support

Cb Protection now supports the use of OneDrive Files On-Demand, a feature which is available beginning with Windows 10 Fall Creators Update. In previous versions of Cb Protection, the agent did not have the ability to detect and track modifications made on another computer to files in the cloud. In order to track these cloud changes, Cb Protection now rehashes all OneDrive files on execution.

Cb Protection does not support custom OneDrive directory paths, which means that the default OneDrive directory path (c:\users\<username>\OneDrive) must be used.

Support for OneDrive Files On-Demand is enabled by default. If you would like to disable it, you will need to disable this feature via the 'disabled_features' agent config property. This can be found in a hidden page within the console at https://<your server>/agent_config.php.

To disable support for on-demand OneDrive files:

1. Log in to your Cb Protection server.
2. Enter the URL for the hidden agent configuration page:
   https://*<yourserverURL>***/agent_config.php**
3. Click the **Add Agent Config** button and fill in the following fields as shown:
   - **Property Name:** disabled_features
   - **Host ID:** 0
   - **Value:** OneDriveFilesOnDemandSupport
   - **Macros:** [leave this empty]
   - **Platform:** Windows
4. Set the Status to **Enabled** and **Save** the changes.

Note: Carbon Black does not recommend storing executables in the cloud, and users should avoid doing so. Due to this recommendation, the Cb Protection agent will ignore the OneDrive directory during initialization. This will leave all of the files inside the OneDrive location as 'unknown'. On every execution of a file in the OneDrive directory, the file will be rehashed and then rules will be applied to block or approve as appropriate. This will have a performance impact as rehashing the file on every execution will take some additional time.

New and Modified Features in v8.0.0

The section New Features in this Release on page 9 describes new features introduced with this patch release. The following sections provide a quick reference to the feature changes made to *prior versions* of v8.0.0 **since v7.2.3**. If you are upgrading to this patch from another v8.0.0 version, you can skip this section.

User Interface Changes

Cb Protection 8.0 provides a visual refresh of the user interface, including:

- **Appearance** – The console incorporates the new Carbon Black corporate colors and includes new icons, buttons, and visual styles. In addition, some navigation items have been moved and text menus replaced by icons.
- **Dynamic scrolling** – Some of the pages within the console have been redesigned to implement a scrolling mechanism that loads more data as you scroll down the page. Where applicable, this has replaced the older, fixed-length paging mechanism.
- **Banner Message Box** – Some of the pages within the console have been redesigned to use a new message box style that spans the width of the page and appears even when you have scrolled to the bottom of the page.

We are approaching the update to the user interface in an iterative way. While the color and icons have been updated everywhere, certain pages are being updated with new elements like dynamic scrolling and the new banner message box as we make core underlying changes to the pages.

See “Using the Cb Protection Console” in *Using Cb Protection* (available as a PDF or through console help) for details about these changes.

Unified Management

If you have multiple Carbon Black Protection servers, Unified Management allows you to designate one server to control many common management functions for itself and any of your other Cb Protection servers. You might choose this option for one or more reasons, including:

- You need to host local Cb Protection Servers in several different regional locations but want to manage some of their functions from a central server.
- You want different types of endpoints (for example, servers, desktops, POS systems) reporting to different servers, but want to have one server manage rules on all of them.
- You have a development server that you use to create custom rules which you then test and deploy to your production server.

Unified Management allows you to view the file inventory for all managed servers through one console. You can also create rules on one server and apply them to some or all of the managed servers. And after a one-time authentication step, a user on the management server can log in to a client server without providing new credentials.

In addition to these features, user interface changes have been made to indicate when feature is affected by Unified Management, and events have been added or modified to track Unified Management activities.

See "United Management of Multiple Servers" in *Using Cb Protection* (available as a PDF or through console help) for more details about these features.

Policy Details Enhancements

Policies can now be renamed on the Policy Details page. In addition, there are new tabs on the Policy Details page that show the rules and settings applicable to the current Policy. These include File Rules, Custom Rules, Memory Rules, Registry Rules, Application Configurations, Publisher Rules, Device Control Settings, Computers (in the Policy), and Advanced Settings.

See "Creating and Configuring Policies" in *Using Cb Protection* (available as a PDF or through console help) for more details about these changes.

Enhanced Role-Based Access Controls

Enhanced Role-Based Access Control provides more granular control over access to console features. In this release, changes to role-based access control include:

- **Users with multiple roles** – In previous versions of Cb Protection, users were assigned to one *group* containing all of that user's permissions. In this release, groups have been replaced by *roles.* Like groups, roles are sets of permissions. However, a user may be assigned as many roles as you choose, and may have roles assigned and removed as needed. For example, you might define a role for a temporary administrator, and assign it to a user when a permanent administrator is on vacation. You can remove that role when the permanent administrator returns without taking away other permissions.
- **AD mapping control –** In previous releases, Active Directory users could be mapped from a fixed set of AD groups to a fixed set of Cb Protection groups, with each user mapped to only one group. In this release, you can create custom mappings. Also, because users can be mapped to multiple roles, each mapping has a "Stop evaluation" option so that an AD user matching that mapping is not assigned any additional roles. **Note:** Mappings from previous releases will be converted to the new, role-based mappings but will preserve the effective behavior of the old mappings.
- **Permissions at the policy level** – In this release, administrators are able to limit user permissions to specific policies. You might consider this to limit access to systems in one region, or systems with a particular function (server, laptop, POS).
- **Changes to User Account page** – You can now view a user's permissions on their account page.

See "Managing Console Login Accounts" in *Using Cb Protection* (available as a PDF or through console help) for more details about these changes.

Workflow Enhancements to Approval Requests

Changes to the Approval Request process were made to help Cb Protection administrators address and resolve requests more efficiently. These changes include:

- Providing more information in the Approval Request detail screen and table, including:
  - The name of the console user who last modified the approval request
  - File prevalence
  - Assessment – This new column displays SRS file trust, SRS threat, all connector verdicts, and publisher trust in one location.
  - External file analysis results

  - Link to Approve files (globally and locally) and Close requests
  - Link to Ban files globally and Close request
- Increasing the number of response actions that can be accomplished directly from the Approval Request table and detail screens
- Eliminating duplicate requests from the same computer/user
- Consolidation of requests for the same file/hash from multiple users, and addition of options to take action affecting all, some, or one of these requests
- Adding a search bar to the Approval Request view to enable quick searches
- Providing a summary panel at the top of the Approval Requests page showing the number of new, open, escalated, and closed requests in the past 24 hours (configurable)
- Providing popup boxes to show information about related requests

Application Identification

A new page provides information about Windows applications discovered by Cb Protection. An Applications on Computers page now shows each instance of an application on each computer.

See “Application Information” in *Using Cb Protection* (available as a PDF or through console help) for more details about these changes.

New Rule Macros

Process Command Line

Cb Protection now supports several new macros that apply a rule when a process command line matches a particular pattern. These new macros include:

- **<CmdLine:X>** - Rule will match if the full command line matches specified pattern X
- **<CmdLineArgumentIdx:X:Y>** - Rule will match if command line contains at least X + 1 arguments, and argv[X] matches pattern Y
- **<CmdLineAnyArgument:X>** - Rule will match if command line contains any argument that matches pattern X.
- **<CmdLineArgumentName:X:Y>** - Rule will match if command line contains argument X and the argv[X+1] matches Y

The macros can always be placed in the "Process pattern" of any Custom, Registry, or Memory rule. For rules that target a process operation (like all Memory rules and process create/terminate Custom rules), the macros will also work in the target pattern. They will not work in the target pattern of an “execute” rule since at the time of execution, the target process/command line is not yet created. The Custom rule *[Sample] Report whenever PowerShell is launched with encoded arguments* provides an example of CmdLine macro usage.

Known Folder Macro

In prior versions, Cb Protection supported rule macros that target CSIDL (constant special item ID list) values to identify special directories in the filesystem. However, starting with Vista, Microsoft deprecated the use of CSIDL’s and started using known folders instead. In this release, a new macro allows direct reference in a rule to any known folder.

The format is <KnownFolder:{GUID}>

A list of known folder GUIDs can be found in the following MSDN article:
https://msdn.microsoft.com/en-us/library/windows/desktop/dd378457(v=vs.85).aspx

For example, to target a user's download directory (FOLDERID_Downloads) in a rule, you could use:
<KnownFolder:{374DE290-123F-4565-9164-39C4925E467B}>

Miscellaneous Macros

- **<HostedService:ServiceName>** - Often custom rules are needed to handle something a particular service is doing within a shared svchost.exe process. In the process pattern of any rule, rather than specifying "svchost.exe", you can now enter <HostedService:*ServiceName*> (replacing *ServiceName* with the name of the shared service). This ensures that the agent only applies the rule to the specificsvchost.exe instance hosting "ServiceName" rather than all svchost.exe instances.
- **<SourceNameOnly>** - This macro can be placed in the "target pattern" field of any custom rule to dictate whether the pattern should only be compared against the source name for rename operations. By default, if this macro is not used in a field, the agent compares the pattern against both the source and destination name, and will match if *either* of the names match.
- **<DestinationNameOnly>** - This macro can be placed in the "target pattern" field of any custom rule to dictate whether the pattern should only be compared against the destination name for rename operations. By default, if this macro is not specified the agent compares the pattern against both the source and destination and will match if *either* of the names match.
  Note: SourceNameOnly and DestinationNameOnly are mutually exclusive.
- **<OnlyIf:ConnectedToServer:*Yes/No*>** - This macro allows you to specify whether or not a rule should only apply when the agent is either connected or disconnected from the server. Specifying "<OnlyIf:ConnectedToServer:Yes>" or"<OnlyIf:ConnectedToServer:No>" in either the target or process pattern will ensure the rule associated with that pattern would only take affect when the connection state is as specified.
- **<OnlyIf:ProcessorArchitecture:*x86/x64*>** - This macro allows you to limit the rule to agents running either 32-bit or 64-bit operating systems.

See "Using Macros in Rules" in *Using Cb Protection* (available as a PDF or through console help) for more details about these changes.

Rapid Configs

Rapid Configs are sets of rules created by Carbon Black that can be used to accomplish tasks such as application optimization, operating system and application hardening, and approval of files delivered by software distribution systems. Some of them are completely pre-configured while others require customization for your environment. They are accessible on a new tab on the Software Rules page.

The rules generated by a Rapid Config all follow a naming convention. They all begin with the name of the Rapid Config followed by a colon and a space and then the name of the rule proper.

Note that the following Updaters have been converted to Rapid Configs:

- Cb Protection Server Tamper Protection
- Cb Response Tamper Protection
- Microsoft SCCM

See "Rapid Configs" in the online Help or PDF version of *Using Cb Protection* for more details about this feature.

Improved Handling of Software Updates during Agent Upgrades

In previous versions of Cb Protection, if an agent upgrade was performed while other software was being installed, files approved via write-approval mechanisms during the upgrade could lose their approval after the agent upgrade was completed. This often affected Windows upgrades.

In this release, server-initiated agent upgrades are deferred if the agent detects that Windows updates are currently being applied. In this case, the agent displays the following message: "Agent Upgrade: Postponed until system updates are completed". This should reduce the occurrence of blocks of system files. One side-effect is that it might increase the time needed for agent upgrades if system updates are frequent.

Note: Upgrades via SCCM or other non-Cb-Protection methods are unaffected by this change.

File Discovery and Approval Mechanism Enhancements

Capture of File Activity before Agent Startup

Cb Protection 8.0 adds a new feature that leverages the Windows' NTFS file system to discover files modified when the agent is not running. The agent uses the NTFS USN Journal to gather a list of modified files so that the agent doesn't need to wait until execution time for the files to be seen. Using this mechanism, files modified while the agent is not active should be discovered shortly after agent startup, increasing the accuracy of the file inventory.

Improved Windows System File Approvals

Cb Protection 8.0 introduces a new mechanism to approve all Microsoft system files. Version 8.0 will locally approve files that have a valid Microsoft signature and reside in the Windows system directory. Also, Cb Protection will locally approve system files that are discovered via typical methods, such as a cache consistency check, execution time discovery, or USN Journal.

Files approved in this way will generate the "File approved (system update)" event, with a new description containing details about how the file was discovered and the OS creation/modification times.

Improved Installer Detection

Agents now recognize more installers that use new and updated installer technologies. Because more installers are recognized, more installers can be approved, and more installations can be completed without extra actions since files from an approved installer are locally approved.

New Rule Type: Expert

In this release, there is a new Expert rule type available for Custom, Memory and Registry rules. Expert rules, as the name implies, are for expert users, and offer more granular control over rule operations and actions. They allow you to combine multiple Actions or Operations into one rule. For example, you can create a single rule that prevents file renames and deletions but still allows file creation and writes.

See "Expert Rules" in the online Help or PDF version of *Using Cb Protection* for more details about this feature. There is also a separate *Using Expert Rules* document on the User eXchange. This is accurate as of v8.0.0 Patch 5, but will be deprecated and not maintained in the future.

Note: Expert rules open up access to very granular control over actions that do not necessarily have user interface equivalents, and they do not have the same error checking features as other rule types. They require much greater care in construction. Contact your Carbon Black representative for assistance if you want to use this new rule type.

Updaters

The Cb Protection 8.0.0 GA release includes updaters that allow updates to Cb Defense for Windows and Cb Defense for Mac. Other updaters may be added in later 8.0.0 releases or via cloud updates.

New Event Types

Cb Protection 8.0 includes new event subtypes in several areas:

- **Agent Notification** – Agent Notification (Other), Agent Notification (Session Change), Agent Notification (Time Change); these events should help you correlate endpoint activity with other system activity such as user logon/logoffs, lock/unlock, etc.
- **File Activity** – File discovered (browser download), File discovered (email attachment), File approved (Unidesk), File downloaded
- **Unified Managemen**t - Unified server added, Unified server error, Unified server modified, Unified server removed, Unified rule overridden
- **Approval Requests and Justifications** – Approval request duplicate created, Approval request escalated, Approval request modified, Justification duplicate created
- **Yara Rules –** Yara Rules Added, Yara Rule Modified
- **Other** - Computer registered, Server upgrade info

See the separate document, *Cb Protection 8.0.0 Events integration Guide*, for complete information about events in this release.

Communication Protocols

The default setting of the agent configuration property winhttp_secure_protocol_flags were changed to SSL 3.0, TLS 1.0, TLS 1.1, and TLS 1.2. Formerly this property was set to WINHTTP_FLAG_SECURE_PROTOCOL_ALL which includes SSL 2.0, 3.0 and TLS 1.0. Carbon Black discourages the use of the SSL 2.0 protocol since it has been deprecated for some time and is known to be more vulnerable to man-in-the-middle attacks. Specifying SSL 2.0 as an option is incompatible with the more secure TLS 1.2 and specifying one prohibits specifying the other. TLS 1.2 is recommended on all platforms that support it (Windows 7 and newer). The new agent default will allow TLS 1.2 to be used.

By default, Windows Server 2016 will not accept connections that attempt to use SSL 2.0 so any agents using the old default winhttp_secure_protocol_flags will not be able to connect to Windows Server 2016 servers without further configuration. This works correctly for the installation of a new 8.0.0 Cb Protection Server on Windows Server 2016. On the other hand, moving an existing install of Cb Protection Server onto Windows Server 2016 requires a change to the winhttp_secure_protocol_flags configuration property for any agents running a previous version of Cb Protection on Windows 7 or earlier before the server is moved to Windows Server 2016. Otherwise, the older agents will be unable to connect using the older WINHTTP_FLAG_SECURE_PROTOCOL_ALL setting.

For more information on the winhttp SSL protocol options see the following articles:

https://msdn.microsoft.com/en-us/library/windows/desktop/aa384066(v=vs.85).aspx

https://blogs.msdn.microsoft.com/kaushal/2011/10/02/support-for-ssltls-protocols-on-windows/

Agent Operating System Support Notes

This section describes special agent operating system support situations for this release. See Agent Supported Operating Systems on the User eXchange for complete agent OS information.

Apple macOS/OSX Agent Support in this Release

A version 8.0 Mac agent is not included in this release. However, version 7.2.3 Mac agents will continue to function with a Cb Protection 8.0 Server.

If you need to deploy additional Mac agents or upgrade existing agents, you can download the latest 7.2.3 Mac agent from the Carbon Black User Exchange. The User eXchange also has instructions that describe how to apply the agent to your server for proper distribution.

Red Hat / CentOS Agent Support in this Release

Linux agents are not included in this release of version 8.0.0. However, 7.2.4 Linux agents will function with a Cb Protection 8.0 Server.

If you need to deploy additional Linux agents or upgrade existing agents, you can download the latest 7.2.4 Linux agent from the Carbon Black User Exchange. The User eXchange also has instructions that describe how to apply the agent to your server for proper distribution.

OS Updates to Windows 10 Anniversary Update and Later

This release includes support for upgrades to Microsoft Windows 10 (Anniversary Update and later) while a Cb Protection agent remains in place. In previous releases, it was necessary to remove the agent when doing major and minor OS upgrades. Please note these important requirements, recommendations, and open issues:

- OS upgrades with the agent in place will work only when upgrading to **Windows 10 Anniversary Update and later**. You must enable Trusted Directory approval of WIM files for in-place agent upgrades to succeed, as described in the next section.
- If you do not have another anti-virus product installed, Windows Defender is enabled by default when you install Windows 10. Consider enabling the Windows Defender updater on the Cb Protection Console (**Rules > Software Rules > Updaters**) to make sure update files for this application are not blocked.
- If you plan to install Windows 10 directly from an ISO, you may need to take additional steps. This case is still being addressed by our engineering team.
- See the *Agent Supported Operating Systems* page on the User eXchange for information about the specific versions of Windows supported for this release.

If you meet the requirements described in this section, you may leave the v8.0.0 agent installed and upgrade to a Windows 10 Anniversary Update or a later supported version from the following versions:

- **Windows 7**
- **Windows 8**
- **Windows 8.1**
- **Windows 10 (previous versions)**

Enabling Trusted Directory Approval of WIM Files

Beginning with Cb Protection v7.2.3, you can enable "crawling" and approval of the contents of Windows Image (WIM) files in trusted directories. Addition of WIM crawling will help increase approval coverage of updates you receive via Windows Server Update Service (WSUS).

One important use of this feature is to enable Cb Protection to support updates to the Windows 10 Anniversary Update and later OS updates on your endpoints without removal of the agent. The procedure described below is a prerequisite for these in-place updates. There may be additional requirements.

See "Approving by Trusted Directory" in *Using Cb Protection* or console help if you have not already set up a trusted directory. If you use multiple trusted directories, the procedure must be repeated for each one in which you want WIM files to be approved.

To allow trusted directory approval of WIM files:

1. Choose or create the trusted directory in which you want to approve the content of WIM files (including those in ISOs). On the system where the trusted directory is located, download and install the Microsoft Windows Automated Installation Kit (AIK). The installation image and instructions can be found in the following locations:
   - For Windows XP and Vista and server equivalents: https://www.microsoft.com/en-us/download/details.aspx?id=10333
   - For Windows 7, 8 and 10 and server equivalents: https://www.microsoft.com/en-us/download/details.aspx?id=5753

   The AIK includes **imagex.exe,** which is required for WIM approval. The download page also includes information and requirements for installing the AIK.
   Note: The locations above include identical versions of imagex.exe. Choosing the one specific to your operating system simplifies installation of AIK.
2. Disable tamper protection on the agent running on the trusted directory server.
   a. On the console menu, choose **Assets > Computers**.
   b. In the Computers table, find the name of the computer hosting the trusted directory, and click on the name or View Details button.
   c. On the Computer Details page, click on **Disable Tamper Protection** in Advanced section of the right menu bar.
3. From the AIK installation location (by default, C:\Program Files\Windows AIK\Tools\amd64\), copy **ImageX.exe** into the agent installation directory (typically C:\Program Files (x86)\Bit9\Parity Agent).
4. Once you copy imagex.exe to the Parity Agent location, you may uninstall the AIK unless you have another reason to keep it on your system.
5. In the Cb Protection Console, approve the ImageX.exe file on the agent hosting the trusted directory:
   a. On the console menu, choose **Tools > Find Files** and search for **ImageX.exe**
   b. In the Find File results, check the box next to ImageX.exe and choose **Approve Locally** or **Approve Globally** on the Action menu.
6. On the Computer Details page for the agent on which you placed ImageX.exe, re-enable tamper protection.

7. Add WIM files to the file types that the agent can "crawl" in a trusted directory:
    a. Navigate to the Support page in the Cb Protection Console by entering the URL: **https://***<yourserveraddress>***/support.php**
    b. Click on the Advanced Configuration tab, and in the Agent Configuration panel, check the box for **Enable Deep Crawl**.
    c. In the next line, **Deep Crawl Files**, add "*.wim" to the end of the list of file extensions if it is not already there. Use a comma to separate the new extension from the previous one in the list. Click **Update** when you are finished.
8. On the console, choose **Assets > Computers**, and locate the computer that has the trusted directory. You must wait until this computer shows **Up to date** in the Policy Status column of the Computers page before proceeding.
9. Copy or move any ISO files and/or separate WIMs you want approved into the trusted directory. The inventory and approval of the contents of these files begins. Completion of this process could take several hours and consume considerable system resources, depending upon your hardware.

For additional info on ImageX.exe, see:

https://technet.microsoft.com/en-us/library/cc722145(v=ws.10).aspx

For additional info on WIM, see:

https://www.microsoft.com/en-us/download/confirmation.aspx?id=13096

Corrective Content

Corrective Content in Cb Protection 8.0.0 Patch 7 Release (Build 2621)

Agent

- The agent's kernel trace file, parity_<agent version number>.etl (e.g., parity_8.1.0.3210.etl), could grow unbounded. In this relese the file is bound by the agent configuration property max_rolling_trace_size_mb value. [EP-3480]
- A single customer received a hotfix that introduced a problem in which a particular sequence of renames and writes could hang or crash the computer. The error is fixed in this version. [EP-4913]
- On startup, previous agents would try to analyze files that were not analyzed prior to shut down. In rare cases, this could lead to stale data that could crash the agent. In this release there is a check for stale data that avoids this crash. [EP-4550]
- An error-handling bug in Yara led to threads hanging and crashing the agent. In this release, the agent detects the impacted error cases without crashing. [EP-4543]
- If the localhost value on a machine was null the agent driver could crash. Validation has been added so to prevent an agent crash in this situation. [EP-4515]
- An installer could execute a rename operation on a file and create a new file with the same name, which in some cases caused the agent to lose track of the original file. This was prevalent with Adobe Reader where the order and timing of operations when Adobe is creating/updating the API files could cause Cb Protection to treat the files as if they were deleted and result in the agent 'rediscovering' the files as unapproved when they execute. In this release, this type of rename and new file action is correctly handled. [EP-4327]

Console

- Several cross-site scripting vulnerabilities were found within the console and corrected. [EP-5256, EP-5209, EP-4546, EP-4544, EP-4538, EP-4516, EP-4520, EP-4331, EP-4523]
- Due to a problem with the tools used to create Cb Protection Help, help displayed from the page-specific (context-sensitive) help buttons displayed the correct topic but did not properly display the help window, including product title and the buttons for search and the table of contents. A tool update from the tool manufacturer corrected this issue. [EP-3146]

Rules

- Users with “Change local state” permission could not locally approve files from the Events page. This has been corrected. [EP-4552]
- Customers with the Ransomware Protection Rapid Config enabled could encounter a BSOD when the agent would scan a file and certain other drivers were running on the system. The conditions causing this problem have been eliminated. [EP-4547]
- Certain rule names caused actions on the rules pages to break. This has been corrected. [EP-4545]
- Past releases contained a race condition involving updating diagnostic counters in two different threads. This would corrupt the counters and trigger a crash. These threads have been synchronized to avoid this problem. [EP-4524]

- In some cases invalid code signing certificates would be accepted as valid and the executable approved by Publisher name. Certificate chain errors are now correctly tracked to avoid accepting invalid certificates. [EP-4521]
- In past releases, files that TMSSClient.exe was copying/quarantining could be inadvertantly be approved. In this release, the Trend Micro OfficeScan process TMSSClient.exe was added to the list of processes that Cb Protection will never consider an installer to avoid this problem. This is sometimes referred to as adding TMSSClient to the "Never Trust" list. [EP-4558]

Corrective Content in Cb Protection 8.0.0 Patch 6 Release (Build 2562)

Agent

- Fixed a problem in which the agent performed unnecessary rule evaluations, leading to significantly increased CPU usage for applications that perform many write operations. This was most commonly seen with browsers such as Chrome and Internet Explorer. [EP-3470]

Corrective Content in Cb Protection 8.0.0 Patch 5 Release (Build 2529)

Agent

- Fixed a problem with the "OnlyIfRegValueIs" macro for rules that had caused the agent to crash. This macro can now be used safely. Note that use of this macro with agents prior to 8.0.0 Patch 5 is not recommended. [EP-1347]
- Improved the kernel's sensitivity to changes in Yara classifications. If an existing Yara classification has changed, the kernel is now notified of that change and immediately starts matching rules that test for that tag. Prior to this change, the kernel was not updated until the agent had some other reason to update the file under consideration. [EP-1531]
- Changed the way the Cb Protection agent opens network files to avoid a possible bypass by way of filenames with trailing spaces. [EP-1860]
- Corrected how certain file read operations were being classified. Occasionally they had been treated as write operations, causing the Cb Protection agent to analyze unchanged files unnecessarily. [EP-2072]
- Removed blocks that prevented the Cb Response sensor from upgrading on the Mac. [EP-2105, EP-2211]
- Ensured that two certificates were added to the certificate store during agent installation. These certificates are used to sign the binaries associated with the Cb Protection agent. These certificates can be identified as follows:

  Code signing root:

  Issuer: VeriSign Class 3 Public Primary Certification Authority - G5

  Thumbprint: 4eb6d578499b1ccf5f581ead56be3d9b6744a5e5

  Timestamp certificate:

  Issuer: GlobalSign Root CA

  Thumbprint: b1bc968bd4f49d622aa89a81f2150152a41d829c

Note that these certificates will typically already be trusted if the machine has received updated roots from Microsoft but on older operating systems they may be missing. These certificates will remain in the trusted root store even if the agent is uninstalled.

- Improved agent performance to reduce the impact of frequent script executions. [EP-2189]
- Identified and fixed an issue that could lead to failure to identify accurate network file paths or resolve short path names properly on windows agent. This issue had caused unanalyzed blocks if the file path that was constructed pointed to an invalid name. [EP-2576]
- Remediated a problem in versions 7.x of the Cb Protection agent where MSI files had been occasionally assigned an incorrect hash type. This caused blocks after an upgrade to versions 8.0.0 before 8.0.0 Patch 5. The remediation ensures that, upon upgrade to 8.0.0 Patch 5 or later, the MSI files are assigned the correct type. Note that this can result in a Cache Consistency check being run when agents are upgraded. [EP-2754]

  Further information about this issue appears in the section Known Issues and Limitations below under the section Rules.

Rapid Configs

- The Browser Protection Rapid Config was modified to include `ParityReporter.exe` as a process that is allowed to make changes to the specified registry settings. [EP-1255]
- Fixed an issue where upgrading the Cb Protection server would cause some Rapid Configs to lose some of their settings. [EP-1435]
- Fixed a bug in the "Cb Response Tamper Protection" Rapid Config such that Cb Protection no longer blocks Cb Response Live Response operations. [EP-1486]

Server Installer

- A Server upgrade will abort if the PHP error log shows Server API errors within the last 7 days. The Cb Protection 8.0.0 Server relies more heavily on the API than prior versions, so if the API is not working, the installer will now prevent an upgrade to 8.0.0 until the API problem has been addressed. [EP-1679]
- Updated the server installer's certificate handling. If an older, self-signed Console certificate is detected which only supports MD5 signature hashing, then the installer will prompt for an upgrade of the self-signed certificate to a more secure algorithm. [EP-1856]

Server

- Addressed a problem with how the Server installer handled the service account name that used to prevent the Server from running after installation. [EP-1150]
- Fixed how the Server collects installed applications from agents such that fewer applications get missed. [52593]
- Recognized applications reported from agents in the Applications Catalog and on the Applications on Computers page that were previously omitted because the install date could not be recognized by the Cb Protection server. These applications are now reported with an empty install date. [EP-1390]
- Fixed how rules are displayed when commas appeared inside tags. [EP-1537]
- Fixed an issue where locked down IIS machines can still receive API requests from the internal server. [EP-1301]

- Fixed a problem where the Console would fail to create a file rule due to a database timeout. [EP-1717]
- Improved the performance of the Find File page when results are sorted by date created. Performance is still best when the default sort order is used. [EP-1305]
- Fixed the erroneous reports of file extensions. Previously, executable files with paths that included a period and without valid extensions displayed part of the path as an extension of the file. [EP-1317]
- Resolved an issue with the generation of API tokens that could cause the Cb Protection Server to lose connectivity with CDC and other unified servers. [EP-1321]
- Fixed an issue where a user's API token remained active even after the user account was disabled. [EP-1406]
- Enabled the download and updating of Yara rules from the Collective Defense Cloud. [EP-1433]
- Changed the "Agent Notification (Session Change)" event to include the User Name in the 'User' column. Previously the User Name was included in the event description. [EP-1472]
- Fixed a problem that prevented simultaneously approving multiple approval requests in the console. [EP-1478]
- Relaxed permissions required for changing a file's local state such that only "change local state" permission is required and "manage files" permission is not required. [EP-1539]
- Fixed an issue that occasionally prevented approvals or custom rule changes from being applied to multiple policies. [EP-1678]
- Fixed a problem in the Console where a database timeout could prevent a file rule from being created. [EP-1717]
- Improved the error handling during file processing so that a Server error is now generated when a timeout or error occurs during processing. [EP-1759]
- Fixed an issue with event rules that prevented the 'move computer' action from working in certain scenarios. [EP-1834]
- Restored the Source Name as a possible choice of column for the Rules pages. This choice had been available in previous versions of Cb Protection. [EP-2017]
- Fixed internal error that was affecting normal server backlog processing. [EP-2045]
- Made it possible to have the forward slash in command-line macros when defining rules. [EP-2060]
- Removed an arithmetic overflow that occurred when calculating the size of larger Cb Protection databases. This caused a number of background tasks to fail, particularly pruning tasks. [2076]
- Fixed issue that could cause premature termination of the nightly prune tasks. [EP-2077]
- Improved the performance of console pages related to the file catalog so that they now work as expected. Previously these pages could time out. [EP-2093]

Corrective Content in Cb Protection 8.0.0 Patch 4 Release (Build 2322)

Agent

- Found and removed a memory leak in the Windows agent's driver which occurred on verifying file signatures. [51333]

- Corrected a problem with the Microsoft Office 2016 Updater that resulted in file blocks after Microsoft Office 2016 updates. [51802]
- Prevented blocks on batch files generated by the GoToMeeting opener application when the GoToMeeting Updater is in use. [51991]
- Corrected a problem with partial certificate chains when checking file signatures. Signed files include some or all of the certificates necessary to validate a file signature. Given a file signed by certificate X missing the full certificate chain as part of the file's signature, the agent will look to the local machines certificate store to fill in the chain. If the necessary certificate is not there, then the agent treats the signature as ineligible for approval due to the partial chain failure. In previous versions, if a different file came in with the same certificate but did had the full chain as part of its signature, then the agent treated the chain as partial even though it could now complete the chain. In this release the agent attempts to reconstruct the full chain each time it encounters certificate X if it has not yet constructed a full chain. [52712, 52792, 52796]
- Corrected a problem where some intermediate and root certificates were not being reported to the server and did not appear in the console. This issue will auto-correct after upgrading agents to 8.0.0 Patch 4 or higher. [52901]
- Made the agent installer more robust so that it can recover from scenarios where the previous version of the product was crashing or failing to shut down. [52702, 52708]
- Strengthened the Rapid Config for Cb Response Tamper Protection to prevent uninstalling Response by means of a command-line flag. [52721]
- Corrected a problem with tracking deletions and renames that only occurs on the newly released Windows 10 Creators Update. [52747]
- Made the agent installer capable of updating rule content (the configlist) when doing a repair install or minor upgrade. In particular, the `B9_CONFIG` command line option is now supported in all install scenarios including clean installs, minor upgrades, major upgrades, and repairs. [52821]
- Supplied an Updater for Cb Response sensors on Linux. [52914]
- Removed a tamper protection block that prevented `msiexec` from creating a `Logs` directory in the agent data directory. (This block event was benign as the directory already existed.) [52916]
- Corrected reports of file discovery dates that were appearing as 1970 in early versions of 8.0.0. An accurate discovery time is now reported. [52919]
- Identified an issue where on rare occasions the agent generated invalid network paths with a format like "\\server\share\subdir\\file.bat" where multiple backslashes separate the filename from the directory path. This could result in unintended blocks on approved files. [52935]
- Identified and removed an issue that on rare occasions caused the agent to stop responding thereby requiring a reboot. [52963]
- Fixed a problem where the agent becomes non-responsive when in excess of 500 devices are attached to its host computer. [53009]
- Strengthened the operation of registry block rules so that a block on a particular key will prevent a rename of all parent keys. This prevents a block on HKLM\Software\Fred\Sally from being bypassed by renaming “Fred” to “Tom”. [53024]

- Provided a status of “Reboot Required” when computers require a reboot to re-enable Windows Update functionality. When upgrading from older 7.x versions, there are cases where the Windows update services (`wuauserv` and `BITS`) needed to be reconfigured in such a way that requires a reboot. For details see the documentation here:

  https://community.carbonblack.com/docs/DOC-5128

  Note that this requirement is not new to 8.0.0 Patch 4. When a computer is in this state then it now shows up on the Computer Details Page with the status "Reboot Required". A healthcheck will also be generated until the computer is restarted. Until it is rebooted, Windows update functionality on the computer will not work. [53026]
- Enabled uploads of files with file paths of arbitrary length. Formerly, there was a 1024 character limit. [53032]
- Prevented templates from being deleted as part of clone pruning. [53040]
- **Note:** The properties of the rule named "Do not treat these processes as .NET applications" have changed. If you modified that rule, your modifications may have been overwritten by these changes. [52786]

Rapid Configs

- Fixed the interface to the Microsoft Office Protection Rapid Config so the parameter labels now update correctly when changing between the Report and Block options. [52746]
- Updated the Windows Hardening Rapid Config to protect applications in the `Windows\SysWOS64` area in addition to the `Windows\System` area by default. [52862]
- Modified the Browser Protection Rapid Config so that it now allows part of the Cb Protection Server (specifically `ParityReporter.exe`) to make expected registry settings. [52929]
- Relaxed the restrictions the Windows Hardening Rapid Config makes on `msmpeng.exe` to allow this executable to modify files. This was done because multiple named services rely on `msmpeng.exe` to be able to do this. [52937]
- Added support for Visual Studio 2017 to the Visual Studio Rapid Config. [52945]
- Changed the defaults for the Browser Protection Rapid Config so that it no longer, by default, reports the launching of `FlashPlayerApp.exe`. [52956]

Server

- Addressed an issue that prevented approving multiple files simultaneously. [1298]
- Improved the performance of the Find Files page. [1297]
- Addressed a problem with agents that prevented them from reporting all code signing certificates to the server. To get the benefit of this fix, agents must be upgraded. [52901]
- Enhanced the logging of errors in using the API. [52714]
- Made the entire row group clickable for expanding and collapsing groups on the console’s table pages. [52741]
- Corrected the expansion of groups on console table pages which did not work correctly in some cases. [52787]
- Allowed the use of double quotes in Custom and Script rules. [52752]

- Made it possible to select the server to search when running Find Files with Unified Management. [52764]
- Identified a problem where agent upgrade errors could be seen on the computers page despite no upgrade ever having been run. Upgrrade failures for other applications were being confused with agent upgrade failures. Now only agent's own upgrade failures will be reported as such. [52791]
- Corrected the removal of rules when using Unified Management. [52800]
- Fixed a number of problems with the Show Individual Files checkbox that appears on the Files on Computers page. Its setting is now recorded with saved views. Grouping and filtering functionality have also been corrected in response to the state of the checkbox. [52812]
- Corrected how the rule that led to an approval request is displayed on the Approval Requests page. [52814]
- Corrected how the Approval Requests page treats requests deriving from custom rules: such requests from different rules are no longer aggregated. [52819, 52833]
- Renamed columns on the new Applications Page. The former Company column supplies the company to which the software was licensed; it is has been renamed "License Owner". The former Publisher column gave publisher information not derived from software signing; to distinguish it from the concept of publisher elsewhere in Cb Protection, it has been renamed "Manufacturer". The former "Install Date" column displayed an installation date as constructed by the software vendor. As the time zone and format of this date differ from software vendor to software vendor, it has been renamed "Estimated Install Date". [52825, 52885, 52893]
- Fixed the "Enable Reputation" checkbox so that checking it is no longer overriden by the policy's initial settings for reputation when creating a policy. [52835]
- Corrected the display of publisher approvals after they have been created. Formerly they were created although the display indicated the opposite; now the display responds correctly when publisher approvals are made. [52837]
- Removed duplication that used to occur when grouping by fields on the Applications Page when the fields take yes/no values. [52844]
- Removed a restriction that prevented manual upgrades from the Computers and Computer Details page for computers that are in the reboot-required state. (Note that there may be other factors that prevent a manual upgrade, e.g., if the agent is at the latest version or if upgrades are disabled or blocked.) [52851]
- Improved the speed with which newly installed applications appear in the Application Catalog and on the Applications on Computers page. Formerly, newly installed applications would not appear until after a computer restart. With this release, they appear within the hour. [52889]
- Corrected the columns shown on the Application Catalog page. Upgrading to 8.0.0 Patch 3 from 8.0.0 Controlled Distribution resulted in only two columns being displayed. By upgrading to 8.0.0 Patch 4 or later, the default columns will be displayed. [52910]
- Prevented Server from crashing as a result of instability in database connectivity. [52926]
- Removed the blank column which appeared when exporting tables to CSV from the console. [52936]
- Fixed a problem that prevented some computers from connecting with the server. [52952]

- Fixed the help link on the Find Files Page. [52961]
- Made it possible for the server to collect more application information for the Application Catalog and Applications on Computers page when using the version of the agent in this update. [52968]
- Fixed a problem with globally approving or banning a file with an already existing rule will now update properly. Previously if a file was approved or banned by policy and the one tried to globally ban or approve it from any of the file pages, it would fail to change the state to global. [52986]
- Made it possible to unify file rules that were present before an upgrade to 8.0.0. [52988]
- Fixed links from the Events page to the Device Details page so that information on the associated device is actually displayed. [52990]
- Fixed a problem where a user with permissions to manage computers in a given policy lost the ability to manage a computer he or she put into Local Approval. [53013]
- Enhanced the Expert Rules page so that deprecated options cannot be created for new rules. They can still be viewed for old rules that use them. [53016]
- Added values from the Excluded column to the preview pop-ups on the File Instances page. [53021]
- Gave all Administrators membership in the "Administrators (Unified Management)" group on upgrade if there are no users currently in that group. This allows previous administrators to configure Unified Management. [53037]
- Supplied a link to the Cb Response console from the Events page when Cb Response appears in the process column of the Events page. [53049]
- Identified a problem with upgrading the Server to 8.0.0 on Windows 2008 R2 where SP1 is required. With this Patch, the Installer detects that SP1 must be installed before the upgrade for Cb Protection can proceed. [53063]
- Removed a cross-site scripting vulnerability from the Computers page. [53058]
- Corrected the filtering by Local State Details on the pages for Find Files and Files on Computers pages. [53066]

Corrective Content in Cb Protection 8.0.0 Patch 3 Release (Build 2146)

Agent

- Prevented Citrix machines from hanging when the agent is installed in a mode other than disabled. [51298]
- Fixed a buffer allocation error that, on rare occasions, could cause a machine running the agent to hang. [51623]
- Corrected a problem that prevented the agent from properly managing script files if the files were discovered (and considered uninteresting) before a script rule affecting them was enabled; setting up script rules before deploying agents is still recommended. [51915]
- Improved the tamper protection that the Cb Protection Agent provides for the Cb Response sensor by preventing unauthorized modification of the Cb Response service keys. [52131]
- Prevented agent crashes that occasionally occurred during computer shutdown. [52413]
- Modified the way the agent imports hashes from a configuration list file so that hashes with upper case letters are now correctly processed. [52480]

- Fixed the behavior of the the Custom Rule “Block powershell scripts that execute memory” (new in v8.0.0) so that it now brings up the correct notifier dialog. [52454]
- Corrected the Custom Rules "Block powershell scripts that execute memory" and "Examine powershell scripts" (new in v8.0.0) so that they no longer block log files and other data files referenced by PowerShell. Note that if you made local customizations to these rules, the updates to correct the previous versions may overwrite your changes. [52455, 52492]
- Extended tamper protection to prevent tampering with the registry keys the agent uses to determine the per-policy setting for starting the agent in safe mode (off by default). [52640]
- Added support for multiple settings for `kernelProcessExclusions` and `kernelFileOpExclusions` on the hidden console page `agent_config.php`. In prior releases, only the first value was recognized. [52661]
- Fixed a problem in which successful agent upgrades pushed through third-party software distribution systems required that the `allow_upgrades` configuration property be set. If used, this configuration property should be disabled after the upgrade as it does open a vulnerability tamper protection would normally protect against. [52707, 52725]
- Corrected a problem in which cache consistency checks run on previous 8.0.0 agents could add some uninteresting (non-executable) files to the agent’s inventory, which could cause blocks if a process tried to map these files into executable memory. If you are upgrading previous 8.0.0 agents, you can run a level 2 cache consistency check after upgrade to purge any uninteresting files added to the inventory from the older agents. [52915, 52934]
- Corrected a problem in which previous versions of the 8.0.0 agent did not properly detect DLL's that were not NX-compatible, which could lead to notifier or `dascli.exe` crashes if third-party security products attempt to inject agent processes with DLL's that violate Data Execution Prevention. If you are upgrading previous 8.0.0 agents, you can run a level 2 cache consistency check after upgrade to make certain the agents’ inventories are correct. [52941]
- Fixed a problem that affected 8.0.0 agents only whereby a specific type of executable was not being added to the agent’s inventory. On upgrading the agent to 8.0.0 patch 3, existing 8.0.0 customers may see blocks on files as they are discovered anew. If desired, these files can be discovered proactively by running a level 3 cache consistency check with the approve new option. [52943]
- Ensured that the agent sends the server information on devices and applications on a more regular basis. [52441]

Rapid Configs

- Restricted the Windows Hardening Rapid Config that appeared in earlier versions of 8.0.0 so that it will only report on files with the following extensions in the the system folder: `exe`, `dll`, `sys`, `msi`, `drv`, `ocx`, and `scr`. [52758]

Trusted Updaters

- Corrected the Google Chrome Trusted Updater so the agent no longer blocks `software_reporter_tool.exe` from running. [52477]
- Provided Tamper Protection for IBM’s BigFix agent. [52715]

Server Installer

- Repaired a problem that prevented upgrades on servers where the database instance uses a case-sensitive collation. [52036]
- Prevented Updaters from being disabled on upgrade. [52122]
- Fixed the server installer so that upgrades should work with a Cb Protection agent running on the machine hosting the server, or if it does not work, the problem is detected early and causes no side effects. [52438]
- Delayed the completion of the installer until the server has completed its upgrade tasks and has become ready to respond to requests; reduced the time required for these upgrade tasks. [52445,52472]
- On server upgrade, prevented agents in policies with upgrades enabled from being upgraded while the global Automatic Upgrade setting was turned off. [52669]
- Reduced duration of server upgrades by removing unnecessary rebuilds of database indexes. [52739]
- Improved progress reporting that occurs during installations and upgrades with more reports of specific database indexes being built. [52770]
- Prevented occasional failures in upgrading the dashboard part of the console by deferring the restart of IIS. [52807]
- Changed the installer to disable Basic Authentication by IIS as part of the installation. If this setting is left enabled, then the Cb Protection API server will be unable to authenticate users and the functionality of the Cb Protection console will be limited. [52878]

Server

- Fixed the inconsistent application of the "Days Disconnected" filter at the top of the Computers page. [48879]
- Provided a warning on revocation of local approval for a file approved by publisher and certificate, because such a file will remain approved. [50682]
- Added initial action information to the SCEP notification type if the action was “quarantined” or “deleted”; allowed actions are not reported as notifications by SCEP. [50687]
- Made it possible to search by “Agent Version” in the search bar of the Computers page. [51145]
- Changed certain Advanced rules from previous release so they open in the new Expert mode. This eliminates a problem where they were being disabled when saved (even without changes) in the current release. [51855]
- Corrected the tamper protection rules for registry keys to make it possible to upgrade the server without disabling tamper protection. [52127]
- Added a dialog to confirm the enabling and disabling of software rules. [52281]
- Corrected the handling of permissions to convert a computer to a template, and to reset the CLI password on the Computer Details page. [52386, 52486]
- The capitalization of the descriptions of events has been made more consistent. [52300]
- Improved the validation of registry paths on the Registry Rules page. [52408]

- Improved the new Approval Request page through changes to the Summary Bar at toward the top of that page. [52440]
- Updated the URL used for Check Point cloud file analysis to `te-s.checkpoint.com` thereby reducing the number of failed file submissions. [52452]
- Added support for two file analysis environments for Check Point: Windows 7 - 64bit and Windows 8.1 - 64bit. [52498]
- Prevented the filters on the Event Rules page from being cleared after navigation away from the page. [52506]
- Enabled local approvals from the Drift Report Details page. [52517]
- Corrected the computation of the total count that appears on console pages showing tabular data. [52527]
- Corrected the Malicious File Detected alert such that it will ignore files that are already banned or approved if it has been configured to do so. [52546]
- Fixed an issue where Wildfire on-premise file analysis would fail when a proxy is used in the environment for external sites. [52547]
- Made it possible to edit the path or file field in a Custom Rule whose current path or file is '*'. [52647]
- Changed text-based filters on console pages that display tabular data. These filters now to default to "is" rather than "contains". [52650]
- Set the settings sections of Rapid Configs to expand by default to make the purpose of this section clearer. [52653]
- Removed an erroneous report of a failure to upload a manifest for a trusted directory which could occur despite the manifest having been successfully uploaded. [52698]
- Provided additional information in event descriptions for unapproved files to make it clear when a file can and cannot be approved by publisher. [52703]
- Improved detection of devices. On rare occasions, some devices did not appear in the console device pages. [52724]
- Fixed a problem with the nightly cleanup process run by the server (the "Daily Prune Task") that could cause it not to finish. [52734, 52750]
- Fixed an issue where failures to upload files for file analysis caused excessive growth in the database and degradation of server performance. [52749]
- Made the time-out used for Cb Collective Defense Cloud communication tasks configurable via the new configuration property `ReporterSRSTaskSQLTimeout`. [52769]
- Removed unnecessary checks for self-signed certificates that could prevent the Cb Protection Console from working with the server API when SAN properties were are used in the console certificate. [52806]

Corrective Content in Cb Protection 8.0.0 CD-4 Release (Build 2024)

Agent

- Corrected a problem with previous 8.0.0 agents where corruption of the boot time protection rules could block all processes on the system and prevent the machine from booting, especially on systems that have a large rule set and are using new expert rules to

test target process information. If you are running previous 8.0.0 agents, you are strongly encouraged to upgrade agents to this version. [52683]

Corrective Content in Cb Protection 8.0.0 CD-3 Release (Build 2023)

Unified Management

- Ensured that the Administrator (Unified Management) user role retains all of the permissions for the standard Administrator role. [52118]
- For Client Servers, added the display of the name of the managing server under Unified Management. [50409]
- Corrected problems with configuring Unified Management from Internet Explorer. [52275]
- Corrected the View Details link for file rules on the managing server so that if a rule is actually on a remote server, the details are requested from that remove server. [52394]

Server

- Enhanced the Expert Rules facility to support customizing notifiers and setting tags for processes. [51469, 52350]
- Corrected the identification of Rapid Config events. Formerly they showed as “Application configuration” events and alerts. [51746, 51867]
- Reduced the number of events generated by the Windows Hardening Rapid Config. [51754]
- Prevented a server upgrade to 8.0.0 from causing the unexpected upgrade of some agents. This occurred even when automatic upgrades had been switched off. [52089]
- Eliminated occasional misleading reports of upgrade errors on successfully upgraded agents. [52224]
- Corrected a problem in which commands on the Action menu did not work properly when multiple files were selected on the File Group Details page. [52227]
- Permitted console users with the View Users role but without the Manage Users role to view their own User Details. [52234]
- Prevented a console user whose Manage Computer permission is limited to a subset of policies from being able to see policies that are not in that user’s permitted subset. [52303]
- Repaired the Ban Globally link on the File Instance details page. [52412]
- Supplied process information on some events that were incorrectly missing such information. [52417]
- Enabled the configuration of notifiers for the Windows Hardening and Browser Protection Rapid Configs. [52428]
- Eliminated timeouts on updating publisher trust through the Cb Collective Defense Cloud. [52495]
- Server upgrades from previous major to this version and subsequent versions of 8.0.0 no longer require that agent tamper protection be disabled on the application server. [52126]
- External web server address can now be used for Agent upgrades. This is configured in the System Configuration page, under Advanced Options. Change is also applied in the Upgrade.xml where "ShareLocation" parameter is now used instead of "ServerIP". [50750]

Agent

- Corrected a race condition on the agent that led to incorrect inventory tracking where file approvals may not take effect. On upgrade, the agent will automatically repair any affected files. [48117]
- Corrected the Cb Protection Agent's tamper protection so that it will now allow the Cb Response sensor to write to the registry. [48974]
- Corrected the behavior of the target pattern field when constructing rules and specifying "*" for the target pattern. [52133]
- Corrected a problem with agent upgrades that prevented the upgrade of agents that had been continuously connected for over twenty days. [52273]
- Closed a resource leak that prevented Cb Protection version 8.0.0 agents from upgrading. [52358]
- Improved the performance of Cb Protection Agents on servers with high login rates. [52379]
- Fixed issues that prevented successful level 1 and level 2 cache consistency checks. [52115]
- Augmented tamper protection so that is no longer possible to delete protected files by identifying them via UNC. [52136]
- Implemented a health check that reports when an agent is installed on a per-user basis, e.g., through SCCM, and should instead be uninstalled and re-installed for all users. [52239]
- Turned off unnecessary of blocks of `ccmexec.exe`. [52280]
- Implemented health check error messages that are now reported when the Cb Protection Agent detects that the volume on which it is installed is short of disk space. Changed reports of upgrade failures due to low disk space to report the cause correctly. [52292]
- Eliminated crashes of the Cb Protection Agent that would occasionally occur when the agent system had a large number of file operations in progress. [52400]
- On machine shutdown, the Cb Protection Agent now shuts itself down with fewer delays. This will result in fewer failed upgrades and service control manager timeouts. [52439]
- An agent crash or hang could occur if you specified a notifier icon download URL that was inaccessible to the agent. Instead, you will receive a system error event noting the download failure [52535]

Corrective Content in Cb Protection 8.0.0 CD-2 Release (Build 1936)

The changes in this release address issues found in previous releases, and include security improvements. The list below is a high-importance subset of those corrections.

Server

- Limited the size of logs of the Server's API interface and provided rolling log and snapshot capabilities to prevent exhaustion of disk space. [45509]

- Provided a tab on Policy Details page that shows the computers in the associated policy. [50204]

- Restricted access to menu items on the dashboard that were formerly not hidden from console users lacking permission to view or use them. [50305]

- Corrected the spacing of the banner on console pages so as to no longer block menu items when the server name or the name of the logged in user is long. [50618]

- Improved performance of console pages displaying grids of data by reducing the number of database queries required to render them. [51808]

- Updated the naming of Cb Response Sensor such that it is no longer referenced as the "Carbon Black Sensor" in events and messages. [51899]

- Fixed the "load more" link on the Firefox browser for larger collections of data. [51918]

- Provided a number of corrections of the operation of the new expert mode for custom rules. [51928, 51910, 52129]

- Corrected event text for custom rules that terminate processes. Previously, these rules generated events that incorrectly reported that a process, such as PowerShell, had been blocked because the executable was banned when the process had actually been started but forcibly terminated. [51732]

Server Installer

- Corrected the installer so that it preserves the policies to which an ATI (Advanced Threat Indicator) has been assigned on upgrade.

- Adjusted the list of required IIS features and permissions for running the Cb Protection Server. [51901]

Agent

- Repaired a problem with the agent's internal datastore that occasionally caused approved files to be blocked. [50597]

- Prevented tampering with the registry keys used by the Cb Protection installer for upgrades. Altering those keys could leave the agent in an inoperable state after upgrade. [50212]

- Scaled back CPU usage exhibited by the Windows agent during cache consistency checks on 8.0.0 CD-1 agents. [51580]

- Removed a health check failure that was triggered if the system ran for more than 180 days, even though nothing was wrong. Provided a new health check if the system time is more than five years from the agent's build time. [51822]

- Repaired a problem with hash-based rules (i.e., a rule to approve, ban, or mark a file as an installer) in which upper case characters were used to specify the hash. Such rules would not take effect under the following conditions:

    - If the hash-based rule was introduced to the agent via a config list import, which occurs on initial install

    - If the hash-based rule was sent to the agent from the computer details "resend all policy information" command

- If the database were corrupted which would trigger a download of all rules from the server.

All such rules are automatically corrected on upgrade to this release. [51846]

- Corrected a problem with approving upgrades to SCCM. [52056]
- Fixed a problem with the "dascli setconfigprops winhttp_secure_protocol_flags <setting>" whereby the command did not take effect immediately but only after the next user login. This command, which is used to test the SSL protocol, may have led to an incorrect assessment of which settings worked. With this fix, testing the protocol will be more reliable. [52062]
- Fixed a problem with agent updates on Windows 8 and Windows 10 machines due to changes the installer used to make for BITS (the background intelligent transfer service) and wuauserv (the Windows update service). These changes caused Windows update problems on those operating systems. With this release, we have stopped changing the configurations of those services and corrected any errors in the configuration of those services. [52326]

Corrective Content in Cb Protection 8.0.0 CD-1 Release (Build 1831)

The changes in this release address numerous issues found in previous releases, and include security improvements. The list below is a high-importance subset of those corrections.

Server

- Improved server performance in many areas, including: tracking of file deletes, renames, and writes; application scalability beyond eight cores; remote desktop login capacity; and significant reduction of upgrade time for large databases.
- Improved the speed of File Catalog display in the console [36622]
- Added command line information to Syslog output for events that include command lines; this was missing in versions 7.2.0 through 7.2.3. [37450]
- Improved the speed of Publisher page display in the console, especially when many publishers are in the inventory. [46183]
- Corrected a problem where a notification to the server from a SCEP-protected computer whose clock was set in the future prevented the import of any other notifications. [46705]
- Upgraded the Advanced Threat Indicators (ATIs) shipped with the server to the most recent versions available at the time of release. [47016]
- Resolved an issue where the agent processed publisher approvals when that agent was in a policy that *did not* have publisher reputation approvals enabled. [47343]
- Corrected an issue where editing multiple event rules at the same time (i.e., opening them in separate browser tabs) could cause edits from one rule to be applied to another rule. [47744]

- Modified the server so that the *update_time_ms* field in the *server_upgrade_history* table correctly reports the time taken to execute the SQL for server upgrade; it previously reported zero in all cases. [48794]
- Corrected the mechanism for applying cloud updates to Advanced Threat Indicators (ATIs) so that they preserve any policy-specific specifications for that feature. [51120]
- Corrected a problem that prevented display of policy names in event tables filtered by either *Malicious File Detected* or *Potential Risk File Detected* subtypes. [51157]
- Addressed an issue where the template tag *'{$host_name}'* in an Elevated Privilege Alert displayed "N/A" instead of the actual host name [51620]

Server Installer

- Added support for .NET 4.6 in the server installer. [43618]
- Added more diagnostic information about IIS installation in the server installation log files. [44315]

Agent

- Improved performance of agents (all platforms) during a policy change. [47353]
- Implemented Windows agent security improvements, including additional validation of data integrity. [36308]
- Addressed an issue where the Windows agent caused long delays in software installations because it was waiting for execution of a network based installer. [41220]
- Improved the security of the Windows agent's handling of system processes that can be promoted as an installer. [42692]
- Updated the Windows agent to recognize installer formats used by Nero and Mozilla, enabling installers using these formats to be "crawled" in a trusted directory and files installed by them to be trusted. [44419]
- Addressed an issue where the Windows agent remained disconnected after the it was put into local approval mode via a timed override key. [45604]
- Resolved a file read issue that impacted the performance of the Windows agent. [46076]
- Reduced the impact of the Windows agent on actions performed on files on network drives. [46961]
- Addressed an issue on Windows agents where frequently scheduled tasks (e.g., every 15 minutes) could consume CPU capacity and make a system appear frozen, especially systems with only 1 or 2 cores. Processing of such tasks is now spread out to be less disruptive to user actions. [47908]
- Addressed an issue where Windows agents would disconnect from the server when the server was very busy. [49652]

Known Issues and Limitations

Agent Installation

- If you are generating installation packages for Linux agents on a pre-8.0.0 server, you should disable package generation before upgrading the server to v8.0.0 Patch 5. Otherwise, the server will fail to generate agent installation packages *after* an upgrade. [52008]

  To disable Linux agent installer generation, log in to the Cb Protection console, go to **https://**<*cbprotectionserver*>**/shepherd_config.php**, and set the **GenerateRedhatInstaller** flag to **false** before upgrading.

  If you already upgraded to v8.0.0 without disabling Linux package generation, you can remediate the problem by running the following SQL:

```
IF EXISTS (SELECT value FROM das.dbo.shepherd_configs
           WHERE name  = 'GenerateRedhatInstaller'
           AND   value = 'true')
EXEC das.dbo.UpdateShepherdConfig @name  = 'GenerateRedhatInstaller',
                                  @value = 'false'
```

  Note: See Red Hat / CentOS Agent Support in this Release on page 17 for important information about Linux support.

- Upgrading Windows 8.1 to Windows 10 using appraiser.sdb and then rebooting will generate the following health check error: "Failed to run kernel health check". This error can be ignored at this time. Other health check errors may also be displayed on upgrades to Windows 10 from earlier versions of Windows operating systems. These health check errors can be ignored at this time, and some of the errors will clear themselves. [49812], [50317]

- In rare cases, agent upgrades may be blocked because older Cb Protection (Bit9/Parity) MSI or MSP packages referenced during upgrade have no global file state. This can occur after a server upgrade from a release *prior to* 6.0.2.228, 7.0.0.1229, or 7.0.1.1109. If you have upgraded from a version prior to those listed, you may have this problem if:
  - Users report that the Cb Protection Notifier shows MSI or MSP blocks after you have enabled agent upgrades.
  - On the console Events page, you notice multiple file block events for the same MSI or MSP files.
  - Agents have an Upgrade Status of "Upgrade Scheduled" but do not ever change to "Up to Date" and have an Upgrade Error of "Agent Upgrade: Unknown error executing" or "Agent Upgrade: Failed executing".

  If this situation occurs, do the following:

  1. **Turn off automatic agent upgrades:** In the Cb Protection Console, choose **System Configuration** on the configuration (gear) menu, and on the System Configuration page, click on **Advanced Options**.
  2. On the Advanced Options tab click the **Edit** button at the bottom of the page, in the Cb Protection Agent panel, choose **Disabled** on the menu, and then click the **Update** button at the bottom of the page.
  3. **Locally or globally approve the MSPs or MSIs that are blocking.**

4. **Turn automatic upgrades back on:** Follow the same procedure as step 1, except choose **Enabled** on the menu.

Note: If you are using a third-party software distribution method to upgrade agents, disable that distribution until you approve the blocking files.

If you encounter this situation and are unsure of whether to approve the blocked files, contact Carbon Black Support.

- Following an upgrade to 8.0.0 Patch 5, you may see tamper protection blocks when `msiexec` attempts to create a `Logs` directory in the agent's data directory. This block event is benign since the `Logs` directory already exists. You will no longer see this block event in subsequent 8.0.0 upgrades.
- Except for certain upgrades to Windows 10, changing the major or minor version of any operating system with an agent in place is not supported, and doing so will produce health check failures and in some cases failure of the upgrade. If you need to upgrade your operating system or you see a health check failure that reports a mismatch between the agent and the build platform, contact Carbon Black Support for remediation recommendations. Service pack upgrades are fully supported and do not cause health check failures.
- 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-1201]
- In VM layering environments (such as Unidesk), do not push updates to the Cb Protection Agent via an update layer. It is possible to push agent updates on an endpoint that has registry data from the prior agent version. If there is a format change for the binary data, the driver can crash because there is currently no method for the driver to know the version of the binary data. [EP-3521]
- On Windows 10, if you uninstall the agent, the paritydriver service might not be uninstalled, and if it remains, it will prevent subsequent installation of an agent on that system. If you encounter this problem, contact Carbon Black Support for assistance in removing the service. [EP-3523]

Agent Behavior

- After agent diagnostic files are generated and then uploaded to the server, they are not deleted from the agent system. This can lead to a significant build-up of large, unnecessary files on the agent system if diagnostics are requested repeatedly from the same agent. It may be necessary to manually remove diagnostics zip files from an agent system in these cases after the files are successfully uploaded to the server. On the Computer Details page for the agent, go to the Advanced section of the right menu bar, and choose **Other Actions > Delete diagnostic files on computer**. [49001]
- The agent currently tracks all the extracted content from the Windows 10 WIM image in the temp directory. A rule to ignore these writes to is not yet functioning properly. [50095]

- On Mac OS X, 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. [26565]

- On OS X and Linux platforms, 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. [26502, EP-805]

- Symantec Endpoint Protection and Cb Protection exhibit a conflict on Mac OS X with regard to Software Update. Some Software Updates are intermittently blocked by the Cb Protection agent as a result. If an update is blocked, it can be approved using the Cb Protection Console and applied again. To avoid future blocks on other endpoints, each blocked update can be globally approved.

  Software Updates blocked by the SEP/Cb Protection interaction produce two events in the Cb Protection events log: a Discovery event with a file written by installd followed by an Execution block (unapproved) event with installd as the process that attempted the execution. [26825]

- On Linux systems, the ext3 file system does not perform journal checksums, which can lead to file system corruption when the disk controller is using out-of-order write caching. In some cases, this can lead to corruption of the Cb Protection Agent database. In order to avoid this, the option "barrier=1" must be added to /etc/fstab for all ext3 file systems.

- If the Notifier Link field causes the launch of an application that is not DEP compatible, the application may not launch when the link is selected, even if the associated application is already running. This occurs because Cb Protection processes require DEP to be enabled as a security measure. Please contact Carbon Black Support for assistance in creating Custom Rules if you encounter this issue. [26943, 26971]

- Known interactions with the VMware vShield Endpoint driver (vsepflt) can cause systems to deadlock in the presence of other filter drivers, such as Cb Protection driver. The vsepflt driver may be loaded on a virtual machine, even when vShield is not in use. Permanently disabling or removing the vsepflt driver will address this issue. Note that VMWare stopped supporting this driver in 2013. [33719, 34411]

- 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. [28824]

- On Mac system, 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. [34305]

- Integration with Cb Response works only on systems running a Cb Protection *Windows* agent. No information from Cb Response sensors (including their presence or absence) is reported from Mac and Linux systems. [39284]

- Improvements to the file analysis system have shown minor performance changes but have led to increased confidence in file classification and analysis. These changes are enabled by default and may lead to an increased initialization time. [51707]

- On computers being upgraded to the 8.0.0 agent, if a script rule had the "Rescan Computers" checkbox enabled, a cache consistency scan will be run and any script files that match that script rule that were not previously encountered by the Cb Protection agent will get approved. Script files already known to the agent prior to upgrade will retain their original state. [EP-2828]

- There is an issue with how the 8.0.0 Windows agent handles situations in which a large amount of data is written to its log. The value in the agent configuration property `max_rolling_trace_size_mb` is supposed to indicate how large in megabytes the agent log is allowed to get before a new log file is created; instead, it indicates when the new log file will get overwritten. As a work around, it is suggested that that this property be set to a value significantly larger than its default of 50. Note that one should *not* set this value to zero. In early versions of the Cb Protection, a value of zero had the special meaning of having the agent never create a new log file. This is not true with version 8.0.0; a value of zero causes each write to the log to truncate. This is another reason giving `max_rolling_trace_size_mb` a large value. [EP-2751]

- When exiting a Timed Override, it is possible that the agent will enter a state that doesn't allow it to send events to the server. This can be resolved by restarting the agent. No events will be lost: after the restart, the agent will send the server the events that it would have sent before restart. [EP-1199]

- On Windows machines, enforcement by the Cb Protection agent of tamper protection can prevent Windows from cleaning up control sets in the registry after a restart. Symptoms of this problem are an accumulation of registry keys in HKLM\System that are no longer needed and tamper protection block events in the console that indicate services.exe was blocked from deleting `ControlSet???`. If you experience this, then disable tamper protection on the agent and reboot your machine. Then re-enable tamper protection. If this is a persistent problem, please contact Support and they can assist you in creating a permanent tamper protection rule that will allow this to occur. [EP-2768]

- On Windows 10, running the command line `sc delete parity` claims to be successful but does not actually delete the service. A restart of the system will restore the service back to its original state. [EP-1251]

- 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. If you experience this, please reach out to Support for the possibility of applying a rule that will provide a mitigation. [EP-3217]

- Under some circumstances, when removable drives are connected to a system running the agent during system restart, duplicate records of a file may be created, triggering errors in the agent logs and error events on the server. This does not affect agent security. [EP-2400]

- A critical system process, for example ntoskrnl.exe, may be tagged by CbP 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 CbP Agent, the issue persists until the system is rebooted or the tag is removed by using expert rule tagging actions. [EP-4988]
- In Windows XP, right-clicking on an “interesting” file and selecting “properties” produces a block, even though that file is not technically being run. [EP-5135]

Integrations

- Check Point integration with local file analysis may stop working due to the fact that the 8.0.0 Cb Protection Server now enforces SSL certificate validation when communicating with the Check Point local appliance. In particular, this affects local self-signed certificates. One way to meet this requirement is to import the self-signed certificate to the trusted people store on the Cb Protection Server machine. This will allow it to pass validation. [EP-2119]

Rules

- When rules targeted to a specific user are exported and then imported, Cb Protection sometimes fails to assign the rule to the user on import. If this happens, assign the rule explicitly to the targeted user *after* import. [47500]

- 7.x agents would incorrectly tag MSI files within our database. In 8.0 we fixed this problem by identifying and setting the tag correctly. However, with this improved tagging, the 8.0 agents could not identify MSI files previously approved with 7.x as the same file post upgrade. As a result the previously approved MSI will be treated as unapproved when launched. 8.0 Patch 5 prevents the loss of the approval state when an MSI is launched. However you will need to repair file rules that have the 7.x associated hash. In order to repair your file rules, please download and deploy the scripts for that purpose that Carbon Black will be posting to User Exchange. [EP-2754]

- When you run a Custom Rule to test an execution block on an OS X 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 OS X operating system. When creating a rule that applies to applications invoked from the typical launching mechanisms of Finder and/or launched on OS X, it is best to also include */usr/lib/dyld* as a potential parent for the application. [47068]

- Some or all memory rules are not supported on certain Windows-based operating systems:
    - Memory rules are not supported on Windows Server 2003 64-bit.
    - Kernel Memory Access rules are supported only on computers running Windows XP or Windows Server 2003 without SP1.
    - Dynamic Code Execution rules are supported only on computers running 32-bit versions of Windows XP, Windows 2003, Windows Vista, and Windows 7 operating systems. On Windows XP, if the system-wide DEP Policy is set to "AlwaysOff", dynamic code execution memory rules cannot be enforced, but Cb Protection will report as though they were enforced. If the policy is set to “OptIn” (the default) or “OptOut”, then these rules will be enforced on systems running XP. [45494]

- When a Custom Rule is used to block writes to a specific file or set of files, and the rule is tested with an editor that creates a backup of the original file, it may appear that the rule is not correctly functioning. This is due to the functionality of certain editors, which may use a rename operation to replace the original file with its backup when any modification is aborted by the user. [29917, 33147]
- This release of Cb Protection does not support targeting script rules at *.dll. Enabling such a rule will cause all processes loading a DLL file to be erroneously classified as script processors. This can cause performance slow-downs and it can use over-approval errors. [EP-1982]
- Software rules based on parent-child relationships between processes do not consistently trigger. [EP-2856]
- When using Unified Management, you might not be able to locally approve files on some linked servers. Attempting to do so triggers the following erroneous message: 'Notice: Cannot create local approval for computer id: X because it is currently in a deleted state.' [EP-3513]
- The Windows Hardening Rapid Config will block Windows 10 upgrades if the Win Verify Trust Section of the Rapid Config is set to “Block” as opposed to “Do Nothing” or “Report.” [EP-4570]

Server Installation and Upgrade

- A Windows account to connect to the Cb Protection Server cannot have braces, single quotes, or double quotes in its password. [52534]
- The server installer does not allow curly braces or quote characters in the SQL password. [EP-4746]
- The Cb Protection Server console requires the Server API to be working in order to function. Starting with 8.0.0 Patch 5, the upgrade process will check whether there are any API errors from the last 7 days, and if it finds any, will inform you that your upgrade has failed a prerequisite check. The API issue must be resolved before upgrading will work. [EP- 1679]
- When Server is upgraded from 7.x versions to 8.0, the IIS private memory size for the default app pool is re-set back to 320Mb which is below Carbon Black’s OER recommendation of 800Mb.

  This will affect deployments with a large number of endpoints that previously had set the IIS private memory size for the default app pool manually above 320Mb and have upgraded the Server from 7.x to 8.0. After the server upgrade, IIS could run out of memory sooner and could return more frequent HTTP 500 errors during Agent upgrades, API and Console usage.

  To remediate, manually set the IIS private memory size for default app pool back to its previous value (usually 800Mb or more) and recycle either DefaultAppPool or IIS itself. [EP-1185]
- If dn entries are incomplete in a prior version of the Cb Protection server’s adrules.xml file, the server can crash when there is an attempt to create an Active Directory policy mapping. [EP-4090 & EP-4088]
- When a Cb Protection server is uninstalled, a message may appear saying that the “system is protected by the Cb Protection agent” even though the agent has already been uninstalled. [EP-4085]

Console

- The Administrator Login Account group can be disabled, and if you have not created another group and account with full administrative privileges, you may not be able to access the Cb Protection Console interface to re-enable it. To correct this, please contact Carbon Black Technical Support team. [40145]
- If you use the "Export to CSV File" feature in a Cb Protection table (such as the Computers page), there is a limit of 25,000 on the number of rows that can be exported.
- Some Rapid Configs require configuration before they can be enabled. These Rapid Configs cannot be enabled from the Rapid Configs tab on the Software Rules page and instead need to be enabled from the Rapid Config details page after providing the required configuration. [52265]
- Block and report events related to the new Ransomware Rapid Config may take over a minute before they are seen on the console. [EP-2393]
- A shortcoming in copying custom, memory, and registry rules can cause a rule to be missing some data. For this version of the software, it is best to create a new rule and copy the individual, relevant fields rather than to copy the rule as a whole. [EP-2111]
- Baseline Drift Reports report on Windows computers only; they do not report on Mac or Linux computers. [EP-2879]
- In the Console, one should be able to create Blocked File Alerts that apply only for computers that are in a specific policy. Such alerts, mistakenly, are applied to all computers. [EP-2920]
- A bulk import of file rules will overwrite any existing file rules with the same hash. [EP-3043]
- Exports to CSV of tabular data from console pages do not render date and time fields consistently with respect to time zone. Some columns are reported as UTC; others use the local time zone. [EP-3157]
- When querying Active Directory for login permissions times out, the Cb Protection console can become unresponsive. [EP-4670]
- A console user account based on Active Directory may be unable to log into Unified Server even when prompted to authenticate. [EP-4660]
- In some cases when the server is set to high-level logging, it does not actually log everything that should be logged in this mode. [EP-4175]
- You cannot locally approve a file that is banned in any policy although you can via the API. [EP-5395]

Application Information

- The names and versions of some applications on the Applications page will appear as empty.
- The install directory of an application is reported as “Default” if the application did not record an `InstallLocation` in the registry when it was installed. If an application did specify an installation directory in the registry, that directory appears as the install directory even if it happens to be the same as the default. [52842]
- The Application Catalog only includes files from Windows computers.
- On the Applications Catalog or Applications on Computers pages, if you group by version number, the groups do not expand. [EP-4152]

Contacting Carbon Black Support

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
Fax: 617.393.7499

Reporting Problems

When you call or e-mail 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)
Document version	For documentation issues, specify the version of the manual you are using. The date and version of the document appear on the cover page of most documents and after the Copyrights and Notices section of longer manuals.
Problem	Action causing the problem, error message returned, and event log output (as appropriate)
Problem severity	Critical, serious, minor, or enhancement