

vmware®

Carbon Black App Control

[View Details](#)



Events Guide

Product Version: 8.5.4

Document Date: November, 2020

Contents

| | |
|--|----|
| Introduction..... | 3 |
| Section 1: Event Specification | 4 |
| Event Fields..... | 4 |
| Timestamp (required)..... | 4 |
| Severity (required)..... | 4 |
| Type (required)..... | 5 |
| Subtype (required) | 6 |
| Source (required)..... | 6 |
| Unified Server Source | 6 |
| Description (required) | 6 |
| IP Address..... | 7 |
| User | 7 |
| File Events..... | 8 |
| Process Events | 8 |
| Process Name, Process Path, Process Key, Process Trust, and Process Threat | 8 |
| Installer, Root Hash | 9 |
| Policy | 9 |
| Additional Fields | 9 |
| Events Table | 10 |
| Section 2: Access to Event Data | 33 |
| Syslog Formats..... | 33 |
| Basic and Enhanced Standard Syslog Formats..... | 33 |
| Basic Syslog Format Message | 35 |
| Enhanced Syslog Format Message | 36 |
| Mapping App Control Events to ArcSight CEF..... | 36 |
| Top-Level Syslog Format..... | 36 |
| Message Format | 36 |
| CEF-App Control Mapping Tables..... | 37 |
| Mapping App Control Events to Q1Labs LEEF Format..... | 40 |
| Configuring QRadar Log Manager | 41 |
| Manual Setup of App Control as Event Source | 41 |
| Top-Level Syslog Format..... | 41 |
| LEEF Format..... | 42 |
| App Control-to-LEEF Mapping Tables..... | 42 |
| Manual Setup of App Control Custom Properties..... | 46 |
| External Event Database..... | 47 |
| Live Inventory SDK..... | 48 |
| Event Output for External Analytics | 48 |
| Archive Files..... | 49 |
| Contacting VMware Carbon Black Support | 51 |
| Reporting Problems | 51 |

Introduction

This document describes the events generated, tracked, and stored by VMware Carbon Black App Control, and the ways you can access these events.

Section 1, *Event Specification*, describes the content, structure and purpose of these events for the benefit of integrators interested in using them outside of the Carbon Black App Control environment. This section includes a comprehensive list of event subtypes and their descriptions.

Section 2, *Access to App Control Event Data*, describes the ways you can access App Control event data outside of the App Control Console user interface. For supported syslog formats, this section shows how event data is mapped.

App Control events provide a critical set of audit data required by many organizations for compliance, legal, and reporting purposes. Among other things, they can show you:

- who is using App Control
- what App Control Server configuration changes have been made
- conditions requiring action (e.g., low disk space or database issues)

For computers running the App Control Agent, events provide information such as:

- file executions that have been blocked due to security rules
- malicious files found by App Control or connected third-party security devices
- new devices found

The App Control API allows programmers who want to write code to interact with App Control using custom scripts or from other applications. As with actions performed through the App Control Console, App Control API activity creates an audit trail. The API user taking the action is identified in the event.

Depending on your role and use case, how you use these events will vary. For example:

- A Help Desk responding to an end user request might be interested in all *block* events for a given computer.
- An IT security specialist responding to an incident might be interested in *new file executions* and events related to *file installation groups*.
- An App Control administrator establishing corporate policies might be interested in classes of events specific to a particular policy interest, such as discovery of new devices or execution of unapproved files (i.e., files neither approved nor banned).

The descriptions in this document will help you locate the specific events you need and filter out those not of interest. If you need more information about App Control features associated with these events, see the *VMware Carbon Black App Control User Guide* for this release, which is available as a PDF file on the Carbon Black [User eXchange](#) and in online help on the App Control Console.

Note: The main table of event types and subtypes in [Table 3](#) describes events as they appear in current versions of App Control v8.5.4.

Section 1: Event Specification

There are two key elements in the App Control event specification:

- the **event fields**, that is, the different types of information available in a single event
- the list of unique **event type/subtype** combinations, shown in [Table 3](#) beginning on page 11.

Event Fields

This section describes the fields that can be in an App Control event. Those shown as “required” can be expected to be present in each App Control event. Other fields are present only for certain events or under certain conditions.

Timestamp (required)

All event timestamps are stored in UTC in the App Control database. The timestamp is the date/time at which the event occurs; that is, it is the time as seen from the source of the event. For example, for server-generated events, it is the UTC time of the server; for agent-generated events, it is the UTC time on the agent computer reporting the event. In the App Control Console, timestamps are displayed according to the time zone setting selected on the General tab of the System Configuration page.

The timestamp for an event corresponds to the date/time when the *App Control Agent or Server* records the event. This means, for example, that a new file discovery during initialization of all files on a new agent computer will show the time the file is first seen by the agent, not when it first arrived on the computer. If the time on the agent computer is not the same as the time on the server, an agent could report a skewed time, including reporting events as happening at a future time.

Note: Although not part of the basic and enhanced Syslog output, a *received* timestamp may appear in other event output from App Control, showing the time the App Control Server received an event.

Severity (required)

Each App Control event has one of five different severity values. [Error! Reference source not found.](#) s hows the severity values listed in order of ascending importance.

Table 1. App Control Event Severities

| Severity | Description |
|--------------|---|
| 6 - Info | Informational message |
| 5 - Notice | Normal, but significant, condition |
| 4 - Warning | Warning condition; worth investigation |
| 3 - Error | Error condition, usually something that requires contact with VMware Carbon Black Support |
| 2 - Critical | Critical condition that requires immediate investigation or action |

Type (required)

This is the top-level, general classification for an event. Each event also has a subtype, which specifically classifies the kind of event it is. [Table 2](#) shows the public event types.

Table 2. App Control Event Types

| Event Type | Description |
|---------------------|--|
| Computer Management | <p>Events related to changes to Computer assets managed by the App Control Server or specific to an App Control Agent. For example:</p> <ul style="list-style-type: none"> - Console management operations like “Computer deleted” and “Computer modified” - Computer/Agent specific diagnostic actions like “Cache check complete” and “Agent synchronization finished” - Template and clone computer management operations - Agent status operations like “Agent restart” and “Agent upgraded” - “Carbon Black EDR sensor status” |
| Discovery | <p>Events related to the discovery or existence of new assets or new actions. For example:</p> <ul style="list-style-type: none"> - Device-related events like “New device found” and “Device attached” - File-related events like “First execution on network” and “New unapproved file to computer” - Events directly related to the metadata retrieved from the Carbon Black File Reputation, Carbon Black’s database of file information. For example, “Malicious file detected” and “Potential risk file detected” - Events related to notification of malicious or potentially risky files from external sources. |
| General Management | <p>Events related to the management of non-user, non-computer and non-policy assets. This includes events related to Meters, Alerts, Baseline Drift reports, Snapshots, and Event Rules. For example, “Alert triggered”, “Baseline Drift Report generated”</p> |
| Policy Enforcement | <p>Events related to the enforcement of any policy or rule on the App Control Agent. For example:</p> <ul style="list-style-type: none"> - File events like “File approved (Updater)”, “Execution block (banned file)”, and “Report write (Custom Rule)” - Device Rule events like “Read block (removable media)” and “Report execution (removable media)” - Registry Rule events like “Write block (Registry Rule)” and “Report write (Registry Rule)” - Memory Rule events like “Access prompt (Memory Rule)” and “Access block (Memory Rule)” <p>Note: This does <i>not</i> include the creation or management of policies. Those events are included under the <i>Policy Management</i> type.</p> |

| Event Type | Description |
|--------------------|---|
| Policy Management | <p>Events related to the management (creation, modification, deletion) of any policy or rule. For example:</p> <ul style="list-style-type: none"> - Policy events like “Policy created” and “Policy deleted” - Software rule events like “Publisher approval created”, “File ban created”, “Trusted User added” and “Custom Rule created” - Device Rule events like “Device approval removed” - Registry Rule events like “Registry Rule created” - Memory Rule events like “Memory Rule modified” |
| Server Management | <p>Events related to the configuration and administration of the App Control Server and database. For example:</p> <ul style="list-style-type: none"> - “Server shutdown”, “License added”, “Server backup stopped”, “Database error” and “Carbon Black File Reputation connection lost” |
| Session Management | <p>Events related to the login activity and management of App Control Console users. For example:</p> <ul style="list-style-type: none"> - Management events like “Console user created” - Login activity like “Console user login” and “Console user logout” <p>Note: App Control Console is the web-based user interface to the App Control Server through which all standard App Control administration takes place.</p> |

Subtype (required)

The subtype corresponds to one (and only one) event type. Subtypes generally map closely to real world use cases and/or App Control product functionality. [Table 3](#) shows the full list of subtypes.

Source (required)

There are two possible values for Source: “System” (the App Control Server or a server component) or a computer name (indicating the event came from an App Control Agent on the named computer).

Unified Server Source

This release includes the ability to manage certain functions on multiple App Control servers from one server. If an event was initiated by a remote server connected via Unified Management, the Unified Server Source field shows the name of that server.

Note: On the console Events page, this field (if available) is displayed only if the logged in user has Unified Management permissions.

Description (required)

The description field is a natural language description of the event. Often, the description will contain information also provided in other fields in the event. This redundancy is intentional; it allows the description to be fully descriptive of the event without the other fields.

[Table 3](#) includes examples (or formats) of descriptions for each unique event subtype, but it does not enumerate all possible event descriptions. Where descriptions contain error messages and other unrestricted content, an exhaustive list is impractical.

Note: Because it can contain sensitive information, including passwords, command line information is included in the Description field for Syslog output from the App Control Server only if command line export is enabled on the System Configuration/Events page in the App Control Console.

IP Address

The IP Address field denotes the IP address of the source of the event. Most, but not all, events have an IP address. For most events, the IP address corresponds to the “Source” field, which is the IP address of the client computer for App Control Agent generated events. This is the IP address of the agent *at the time of the event*, not necessarily the current IP address of the agent.

Events generated by App Control Console activities report the IP address of the machine on which the user is accessing the console. For example, “Console user login” and some “File approval created” events contain the IP address of the computer on which a console user performed those actions.

Most events generated by the App Control Server, Reporter and the database itself (whose source is “System”) do not have an IP address. This includes, for example, events such as “Alert triggered” and “Server errors”. In those cases, the IP address is unnecessary, since it is always the same. Exceptions to this rule are Server and Reporter start and stop events, which contain IP address of the Server and Reporter for diagnostics purposes.

User

The User field contains either the user that was active on the agent computer (Source) at the time of the event, or the Console User in the case of events generated by console activities. There are cases in which an event cannot be attributed to either a console or a logged in user on an agent system:

- In some cases, the user name will be “System”.
- The User field might be empty when there is no user account to attribute to the event. This occurs for agent-generated Computer Management events like “Agent restart” and “Agent Policy updated”. Those events are initiated by the App Control Agent itself and therefore have no associated user.
- In some cases, the User field will be “<unknown>” because a user cannot be determined. For example, it would be <unknown> for the Discovery events “Device attached” and “Device detached”. When devices are attached or detached from a computer, App Control tries to determine which user is currently “active” at that time. If an active user cannot be determined – for example, if there is no one currently logged in – App Control will use the special string “<unknown>” for User.

If you are using Unified Management of multiple servers, the “user” identified for actions performed on client servers through the management server is not necessarily the user currently logged into the console. The account used to *authenticate* the connection between the management server and the client server appears as the user.

File Events

The following events relate to a specific file:

- **File Extension**
- **File First Execution Date**
- **File Hash**
- **File Name**
- **File Path**
- **File Prevalence**
- **File Publisher**
- **File State**
- **File State Reason**
- **File Threat**
- **File Trust**

When the event relates to a specific file (e.g., “Execution blocked”, “New unapproved file”), the File Hash, File Name, and File Path fields will be completed with the file-specific information that is available. Not all file events will have these fields completed. For example, an “Execution blocked (still analyzing)” event, will not have a file hash. Policy Management events, like creating approvals and bans, also contain File Hash or File Name data when available and applicable.

When the File Hash is available, it is a SHA-256 hash. The File Path does *not* end with a trailing slash.

File State provides the global state of the file associated with the event (Approved/Unapproved/Banned) and File State Reason provides additional details behind the global state of the file associated with the event. File Prevalence lists the number of computers on which the file associated with an event appears.

If Carbon Black File Reputation data is enabled when the file event is generated, File Trust and File Threat information is included in the event if it is available.

Process Events

The following events relate to a specific process:

- **Process**
- **Process Hash**
- **Process Key**
- **Process Name**
- **Process Path**
- **Process Prevalence**
- **Process Threat**
- **Process Trust**

Process Name, Process Path, Process Key, Process Trust, and Process Threat

Several Process fields are used within events generated by the App Control Agent. Most of them are similar to the File fields, except that they describe the running process that caused an event to be generated rather than the file that is the target of an action. For example, when a file execution is blocked and the “Execution block” event is generated, the event will include the Process Name field with the file name of the program that tried to launch the blocked file.

The Process field provides the full path and name of the process associated with the event and Process Prevalence lists the number of computers that have the process associated with an event.

Typically, the process fields appears in Discovery events or Policy Enforcement events but also can be part of certain subtypes of other event types.

If Carbon Black File Reputation data is enabled when the file event is generated, Process Trust and Process Threat information is included in the event if it is available.

Process Key is a unique, proprietary key identifying the instance of the process on a specific computer.

Note: A “Process” field (without any additional term) is also in events exported to Syslog and archives. This field contains the name and full path, and is used for compatibility with pre-7.2.0 agents and events. Another field, Process Hash, is exported only in archived events (see [Archive Files](#) on page 49).

Installer, Root Hash

Installer and Root Hash are used within some events generated by the App Control Agent.

The Installer field contains the name (*not* the path) of the file that *created* the file referenced by a File Name and/or File Hash – in other words, the root parent or “installer” of that file.

In many cases, the Installer is the same as the Process Name, but not always. For example, for file approval events, the process running is often (by definition) the same as the installer that is approving the file being written. In the case of execution block events, the process running may or may not be the same as the process that wrote the file in the first place.

For example, consider what happens when the installer *setup123.exe* writes the file *myapp.exe*. When *myapp.exe* is first written on a computer running an App Control Agent, a “New file on network” event is generated, and both its *Process Name* field and its *Installer* field reference *setup123.exe*. If *myapp.exe* is later launched from a command prompt and is blocked, the *Process Name* field may be *cmd.exe* while the *Installer* field is still *setup123.exe*.

The Root Hash field is the SHA-256 hash value of the Installer file.

Policy

The Policy field is used within events generated by the App Control Agent. It contains the name of the App Control security policy in effect on the agent at the time of the event.

Additional Fields

The following additional fields are not mandatory but may appear in events:

- **Ban Name** – For block events, name of the ban that blocked the file.
- **Computer ID** – A numeric ID for the computer associated with the event (0 for system). Increments by one for each computer registered with the server.
- **Computer Tag**– An optional text string you can add to identify groups of computers that you might want to get reports about or treat in a particular way. A tag offers an alternative to policies as a way to identify groups of computers. Tags may be set on the Computer Details page for one computer or on the Computers page Action menu for multiple computers.
- **Config List Version** – Version number of the Config List associated with an event. The Config List is the set of rules delivered to agents.
- **Date Received** – Timestamp when the event was received by the App Control Server (in UTC).
- **Indicator Name** – Name of the threat indicator associated with the event, if present. Same as rule name when present.
- **Indicator Set** – Name of the threat indicator set for the indicator associated with the event, if present.
- **Operating System Details** –Full OS name, the build, and service pack level.
- **Platform** – Platform of the computer associated with the event (Windows, Mac, Linux).
- **Rapid Config** – The name of the Rapid Config associated with the event, if any.
- **Rule Name** – The name (as it appears in the console) of the rule associated with the event. This includes both user-created rules and built-in rules, such as *Prompt on unapproved executables*.
- **Unified Source** – The name of the unified server associated with the event, if any.
- **Updater** – The name of the updater associated with the event, if any.

Events Table

[Table 3](#) lists all events types and their unique subtypes in App Control v8.5.4. New or changed events are shown with the following legend:

Note: There were no new or changed events in 8.1.10.

- 📄 Changed for v8.5.0 (e.g., CB Protection changed to Carbon Black App Control)
- 🕒 New for v8.1.8; type and subtype shown in bold
- New for v8.1.6; type and subtype shown in bold
- Changed for v8.1.6 (e.g., type, subtype, severity, description, triggering condition); type and subtype shown in bold
- New for v8.1.4; type and subtype shown in bold
- Changed for v8.1.4 (e.g., type, subtype, severity, description, triggering condition); type and subtype shown in bold
- ▲ New for v8.1.0; type and subtype shown in bold
- △ Changed for v8.1.0 (e.g., type, subtype, severity, description, triggering condition); type and subtype shown in bold
- ✦ New for v8.0.0
- ◇ Changed for v8.0.0

For information about event changes prior to v8.0.0, see the [Bit9 Security Platform v7.2.3 Events Integration Guide](#) on the Carbon Black [User eXchange](#).

In the Example Descriptions/Comments column, the descriptions show the text and/or format of the descriptions for each event. Variable information is shown with the convention “\$variabledata\$”. So for example, where the actual Description field for an event would show the name of a computer (e.g., “Laptop-5”), the Description column in this table shows “\$computer\$”. Variables that use parameters from App Control, where these parameters are not commonly known objects outside of the App Control context, are shown in the format “\$param1\$”, “\$param2\$”, etc. You can view the actual event output from App Control or view the Events page through the App Control Console to see real-world examples of these parameters. For example, an event shown in this guide as “Computer \$computer\$ discovered new file '\$filePathAndName\$' [\$hash\$].” might look like this in the console:

| Subtype | Description |
|---------------------------------|--|
| New unapproved file to computer | Computer MYCORP\LT-5 discovered new file 'c:\windows\system32\custom' [30374...56D8D]. |

If you have upgraded from a previous version of this product, note the following changes that affect multiple events:

- Several product name changes in version 8.5.0 have affected certain event subtypes and descriptions:
 - CB Protection is now Carbon Black App Control.
 - CB Response is now Carbon Black EDR.
 - Carbon Black Collective Defense Cloud is now Carbon Black File Reputation.
- Several product name changes in version 8 have affected certain event subtypes and descriptions:
 - Parity Server/Bit9 Server is now CB Protection Server.
 - Parity Agent/Bit9 Agent is now CB Protection Agent.
 - Parity Console/Bit9 Console is now CB Protection Console.
 - Parity Knowledge Service/Bit9 Software Reputation Service is now Carbon Black Collective Defense Cloud.
- Numerous other changes, including some user interface names, have been made since the 7.x product cycles.
- Beginning with v7.2.1, what was labeled “Priority” was changed to “Severity”.
- In v8.1.0, capitalization of many subtype names was changed for consistency.

Table 3. App Control 8.5.4 Event Types and Subtypes

| | Type | Subtype | ID No. | Severity | Example Descriptions/Comments |
|----|---------------------|-----------------------------------|--------|----------|---|
| | Computer Management | Agent bulk state change finished | 412 | Info | Computer '\$computer\$' completed the state transition of all files from '\$param1\$' to '\$param2\$'. Note: Parameters 1 and 2 can be 'Unapproved' or 'Locally Approved'. |
| | Computer Management | Agent bulk state change requested | 413 | Info | '\$userName\$' requested state transition of all files on computer '\$computer\$' from '\$param1\$' to '\$param2\$'. Parameters 1 and 2 can be 'Unapproved' or 'Locally Approved'. |
| | Computer Management | Agent config modified | 435 | Notice | Agent configuration property '\$param1\$' was created as '\$param2\$' (\$param3\$) by '\$username\$'. Agent configuration property '\$param1\$' was modified to '\$param2\$' (\$param3\$) by '\$username\$'. Agent configuration property '\$param1\$', value '\$param2\$' (\$param3\$) was deleted by '\$username\$'. Examples: Computer retrieved Notifier Logo: Source[\$param1\$] Attempts[\$param2\$]. Agent configuration property 'KernelWriteExcludePattern' was modified to '/opt/apps/*' (Enabled) by 'bjones@mycorp.local'. Agent configuration property 'protocol_message_versions (Linux)' was modified to 'protocol_message_versions=1:4,2:1,3:1,5:4,6:7,7:5,8:3,9:4,10:1,11:1,12:2,13:1,14:1,15:2,16:1,18:1' (Disabled) by 'rgomez@mycorp.local'. |
| FD | Computer Management | Agent database error | 432 | Error | Carbon Black App Control Agent had to restore its primary database cache. Carbon Black App Control Agent had to rebuild its primary database cache and now has to re-initialize. Carbon Black App Control Agent detected a cache integrity problem. Unknown error initializing database pool. Carbon Black App Control Agent had to restore its primary database cache. Carbon Black App Control Agent had to rebuild its primary database cache and now has to re-initialize. Carbon Black App Control Agent failed to upgrade its database. Carbon Black App Control Agent failed to connect to its cache database. |

| | Type | Subtype | ID No. | Severity | Example Descriptions/Comments |
|--------|---------------------|-------------------------------------|--------|----------------------------|--|
| | | | | | Carbon Black App Control Agent failed to read config list from file. Carbon Black App Control Agent failed cache verification. Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0. |
| | Computer Management | Agent deleted events | 414 | Notice | Computer '\$computer\$' deleted \$param1\$ events. Note: Param1 is a numeric value. |
| | Computer Management | Agent Enforcement Level changed | 407 | Notice | Computer '\$computer\$' changed Enforcement Level from '\$param1\$' to '\$param2\$'. Note: Parameters 1 and 2 are one of the Enforcement Levels or "Local Approval". |
| Ⓜ | Computer Management | Agent error | 431 | Error | Unsupported kernel [\$kernelversion\$] running. Agent will not track files. Carbon Black App Control Agent was unable to communicate with the kernel. Agent may be unprotected Unable to connect to the Kernel. Agent will not track files. Computer failed to receive Notifier Logo: \$logoFilePath\$. Free space on Carbon Black App Control Agent drive is low: Drive[\$letter\$:] Available[\$param1\$] Total[\$param2\$] Free[\$param3\$] Threshold[\$param4\$] Upload failed: Retry limit exceeded. File upload canceled for file '\$filePath\$'. Attempts[\$param\$] Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0. |
| ▲ | Computer Management | Agent FIPS status changed | 851 | Info | FIPS status has changed on computer '\$computer\$' from '\$param1\$' to '\$param2\$'. |
| Ⓜ | Computer Management | Agent health check | 447 | Info/ Error/ Warning | Carbon Black App Control Agent is healthy. Options[\$param1\$]. Carbon Black App Control Agent failed a health check. ErrorsFound[\$param2\$] Options[\$param1\$] Carbon Black App Control Agent detected a problem: \$param1\$. \$param2\$ Timestamp of events from computer \$computer\$ are \$param1\$ day(s) in the \$param2\$ Timestamp of events from computer \$computer\$ are within expected range Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0. |
| | Computer Management | Agent health check request | 457 | Info | User '\$userName\$' requested health check for computer '\$computer\$'. |
| Δ + | Computer Management | Agent notification (other) | 1019 | Info | Service control notification on '\$computer\$': \$param1\$. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ + | Computer Management | Agent notification (session change) | 1018 | Info | Session change on '\$computer\$': \$param1\$. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ + | Computer Management | Agent notification (time change) | 1017 | Info | System time change on '\$computer\$': \$param1\$. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| ○ Δ | Computer Management | Agent Policy changed | 406 | Notice | Policy change was scheduled for computer '\$computer\$' from '\$param1\$' to '\$param2\$'. Change Note: Subtype capitalization was changed in v8.1.0. Description was changed in v8.1.4. |
| Δ | Computer Management | Agent Policy updated | 408 | Info | Computer '\$computer\$' updated Policy from version '\$param1\$' to '\$param2\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| | Computer Management | Agent requires upgrade | 415 | Notice | Agent polled from '\$ipaddress\$'. Agent Version(\$param1\$). Agent needs to upgrade to latest version. |
| Ⓜ | Computer Management | Agent restart | 405 | Info | Carbon Black App Control Agent has started, version \$param1\$. Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0. |
| Ⓜ | Computer Management | Agent shutdown | 404 | Info | Carbon Black App Control Agent was stopped because of a system shutdown. Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0. |
| Ⓜ | Computer Management | Agent synchronization finished | 411 | Info | Computer '\$computer\$' finished resynchronizing its local state with the Carbon Black App Control Server. (Reason: '\$param1\$'). |

| | Type | Subtype | ID No. | Severity | Example Descriptions/Comments |
|---|---------------------|---------------------------------|--------|----------|--|
| | | | | | <p>Note: Param1 is one of the following: 'Agent queue size grew too large', 'Server request during agent initialization was deferred', 'Server request during agent cache consistency scan was deferred', 'Server request', 'Agent did not have enough history', 'Protocol error', 'Agent CLI Request'</p> <p>Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0.</p> |
| O | Computer Management | Agent synchronization requested | 418 | Info | <p>User '\$username\$' has requested resynchronization of computer '\$computer\$' with the Carbon Black App Control Server.</p> <p>Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0.</p> |
| Ⓜ | Computer Management | Agent synchronization started | 410 | Info | <p>Computer '\$computer\$' started resynchronizing its local state with the Carbon Black App Control Server (Reason: \$param2\$).</p> <p>Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0.</p> |
| | Computer Management | Agent uninstalled | 421 | Notice | Agent has been uninstalled from computer '\$computer\$' |
| | Computer Management | Agent upgraded | 409 | Info | Computer '\$computer\$' changed agent version from '\$param1\$' to '\$param2\$'. |
| Ⓜ | Computer Management | Automatic resynchronization | 425 | Info | <p>Carbon Black App Control Server scheduled an auto resync on '\$computer\$' because agent appears to have gone back in time (\$param1\$/ \$param2\$).</p> <p>Note: Param1 is the server's expected sequence number of an action. Param2 is the sequence number sent by the agent, which can be used for diagnostic purposes with Carbon Black Support.</p> <p>Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0.</p> |
| | Computer Management | Cache check complete | 416 | Info | <p>Cache consistency check stopped Level [\$param1\$] \$param2\$</p> <p>Cache consistency check complete: \$param1\$ optimizations made, \$param2\$ corrections.</p> <p>Note: Param1 is cache consistency level. Param2 is a series of values for diagnosis of what was done during the check, and also indicates whether the check ran to completion ("Successful[1]") or stopped before completion ("Successful[0]").</p> |
| | Computer Management | Cache check error | 417 | Warning | Cache consistency error number '\$param1\$', file '\$param2\$'. |
| | Computer Management | Cache check start | 426 | Info | Cache consistency check at level '\$param1\$', flags '\$param2\$' started. |
| | Computer Management | Cache consistency check request | 453 | Info | <p>User '\$userName\$' requested a cache consistency check Level[\$param1\$] Options[\$param2\$] for computer '\$computer\$'</p> <p>Note: Param1 is the consistency check level chosen by the user and param2 indicates any option checkboxes chosen, such as "Full scan of new files".</p> |
| ◇ | Computer Management | Carbon Black EDR sensor status | 458 | Info | <p>Carbon Black EDR Sensor Version '\$param1\$' installed and '\$param2\$'.</p> <p>Carbon Black EDR Sensor is not installed.</p> <p>Note: param1 is the Carbon Black EDR sensor version; param2 is the sensor state (e.g., 'Running').</p> <p>Change Note: Prior to v8.0.0, the event subtype was "Carbon Black sensor status".</p> |
| | Computer Management | CLI executed | 429 | Notice | The CLI command "\$commandname\$" was executed. |
| | Computer Management | CLI password reset | 403 | Notice | The CLI password for computer '\$computer\$' was reset by '\$username\$'. |
| | Computer Management | Clone orphaned | 446 | Info | Clone computer '\$computer\$' was orphaned due to deletion of template '\$param1\$'. |
| | Computer Management | Clone registered | 445 | Info | Computer '\$computer\$' was registered as a clone of template '\$param1\$'. |
| | Computer Management | Computer added | 400 | Info | New computer '\$computer\$' with Policy '\$policyName\$' registered from '\$ipAddress\$'. Agent Version (\$param1\$). |
| | Computer Management | Computer deleted | 401 | Info | Computer '\$computer\$' was deleted by '\$username\$'. |
| | Computer Management | Computer modified | 402 | Info | Computer '\$computer\$' was modified by '\$username\$'. |

| | Type | Subtype | ID No. | Severity | Example Descriptions/Comments |
|---|---------------------|--|--------|----------|--|
| | | | | | Computer '\$computer\$' was moved into the Policy '\$policyName\$' by '\$username\$'. Computer '\$computer\$' was modified by '\$username\$' to use automatic Policy assignment. Computer '\$computer\$' was restored to its previous Policy by '\$username\$'. Computer '\$computer\$' was scheduled for re-registration by '\$username\$'. Duplicate computer '\$computer\$' with address '\$param1\$' was re-registered. Computer from '\$param1\$' changed its name from '\$param2\$' to '\$param3\$'. Agent upgrade for computer '\$computer\$' was requested by '\$username\$'. |
| | Computer Management | Computer reboot request | 441 | Info | User '\$username\$' requested reboot of computer '\$computer\$'. |
| + | Computer Management | Computer registered | 459 | Info | Computer '\$computer\$' registered with the server. \$param1\$ users are currently logged-in to the computer. |
| | Computer Management | Configuration changed | 434 | Info | Disk configuration change detected: \$param1\$ volumes added; \$param2\$ volumes removed. |
| | Computer Management | Configure agent dumps | 452 | Info | User '\$username\$' changed agent dump configuration from \$param1\$ to \$param2\$ for computer '\$computer\$'. |
| | Computer Management | Debug level set | 451 | Info | User '\$username\$' set debug level for computer '\$computer\$' from '\$param1\$' to '\$param2\$' for \$param3\$ minutes. |
| D | Computer Management | Diagnostic file deletion request | 454 | Info | User '\$username\$' requested deletion of diagnostic files from computer '\$computer\$'. Change Note: Prior to v8.1.0 this subtype was "File deletion request". |
| | Computer Management | Duplicate computer registration | 433 | Warning | Error registering computer '\$computer\$' from \$ipaddress\$ [\$param1\$]: unique agent id duplicates that of computer \$param2\$ from \$param3\$. |
| ▲ | Computer Management | File deleted | 460 | Info | File 'test123.bat' [FBAD9...34F00] was successfully deleted from MYCORP\LAPTOP3 |
| ▲ | Computer Management | File deletion failed | 461 | Error | If the deletion failed because it was a file from a protected publisher: File deletion failure of 'emet_gui.exe' [2024F...41CCD] from MYCORP\LAPTOP3. Error: Microsoft File If the deletion failed because the agent version doesn't support server-based deletion: File deletion failure of 'emet_gui.exe' [2024F...41CCD] from MYCORP\LAPTOP3 because this Agent version doesn't support it. If the deletion failed because the file is no longer present on the computer and not in its inventory: File deletion failure of 'tryme.bat' [76C7F...BD915] from MYCORP\DESKTOP8. Error: Delete Error[C0000034] |
| ▲ | Computer Management | File deletion processed (file not found) | 466 | Info | If a file is exists in a computer's inventory but is not on disk: File deletion processed with file not found for [EADB7...12F06] from MYCORP\DESKTOP9 |
| ▲ | Computer Management | File deletion requested | 464 | Info | If the request was to delete a file from one computer: User 'admin' requested file deletion of all instances of [2488C...558F1] from MYCORP\DESKTOP6. If the request was to delete a file from all computers: User 'admin' requested file deletion of all instances of [FBAD9...34F00] from 100 computer(s). If the request was to delete a file came from an Event Rule: User 'System' requested file deletion of all instances of [81027...576DA] from MYCORP\DESKTOP6. |
| Ⓜ | Computer Management | File process error | 423 | Error | Agent on computer '\$computer\$' is unable to process required update '\$param1\$' from Carbon Black App Control Server. Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0. |
| Ⓜ | Computer Management | File receive error | 422 | Warning | Agent on computer '\$computer\$' is unable to download required update '\$param1\$' from Carbon Black App Control Server. |

| | Type | Subtype | ID No. | Severity | Example Descriptions/Comments |
|--------|---------------------|--------------------------------------|--------|----------|---|
| | | | | | Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0. |
| | Computer Management | File upload canceled | 438 | Info | User '\$username\$' canceled upload of file '[hash\$]' from computer '\$computer\$'. User '\$username\$' canceled upload of file '\$filePath \$' from computer '\$computer\$'. |
| | Computer Management | File upload completed | 439 | Info | Upload of file '[hash\$]' from computer '\$computer\$' completed. Upload of file '\$filePathAndName\$' from computer '\$computer\$' completed. |
| | Computer Management | File upload deleted | 449 | Info | User '\$username\$' deleted uploaded file '[hash\$]'. User '\$username\$' deleted uploaded file '\$filePathAndName\$'. |
| | Computer Management | File upload error | 440 | Error | Upload of file '[hash\$]' from computer '\$computer\$' failed because of error '\$description\$'. Upload of file '\$filePathAndName\$' from computer '\$computer\$' failed because of error '\$description\$'. |
| | Computer Management | File upload requested | 437 | Info | User '\$username\$' requested upload of file '[hash\$]' from computer '\$computer\$'. User '\$username\$' requested upload of file '\$filePathAndName\$' from computer '\$computer\$'. Upload of file '[hash\$]' from computer '\$computer\$' was requested by Event Rule '\$ruleName\$'. |
| | Computer Management | Installer rescan requested | 424 | Info | User '\$username\$' has requested rescan of installers on computer '\$computer\$'. |
| | Computer Management | Local agent cache copy request | 455 | Info | User '\$userName\$' requested local copy of agent cache for computer '\$computer\$'. |
| | Computer Management | Lockdown all computers | 427 | Warning | Lockdown All button pressed by '\$username\$': '\$param1\$' computer(s) have been moved to High Enforcement level. |
| | Computer Management | Prioritize updates request | 450 | Info | Updates prioritized for computer '\$computer\$' by user '\$userName\$'. Prioritization of updates removed for computer '\$computer\$' by user '\$username\$'. |
| D | Computer Management | Resend all Policy rules request | 456 | Info | User '\$userName\$' requested all Policy rules be resent to computer '\$computer\$'. User '\$userName\$' requested all Policy rules be resent to computer '\$computer\$' using shared file. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ Ⓜ | Computer Management | Security Alert | 448 | Warning | Unauthorized connection attempt: Pid[\$processId\$] Address[\$IPaddress\$] to the Notifier client interface The \$fileState\$ file '\$filePathAndName\$' '[hash\$]' is set to run automatically: '\$param2\$'. Notes: fileState is the state of the file in Carbon Black App Control (e.g., Unapproved or Banned). Param2 is a description of the file source (e.g., Service [Microsoft Network Inspection]). The case referred to in the second description does not occur for agents in Low enforcement, and only once per file unless there is a reboot. Change Note: Capitalization of the subtype was changed in v8.1.0. Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0. |
| Δ | Computer Management | Tamper Protection changed | 428 | Warning | User '\$username\$' has disabled Tamper Protection on computer '\$computer\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| | Computer Management | Template created | 442 | Info | User '\$username\$' has converted computer '\$param1\$' to template '\$computer\$'. |
| | Computer Management | Template deleted | 444 | Info | User '\$username\$' has deleted template '\$computer\$'. |
| | Computer Management | Template modified | 443 | Info | User '\$username\$' has modified template '\$computer\$'. |
| | Computer Management | Temporary Enforcement Level override | 419 | Warning | A temporary override to place computer '\$computer\$' in Enforcement Level '\$param1\$' for '\$param2\$' minute(s) has been accepted. |
| | Computer Management | Temporary Enforcement Level restore | 420 | Notice | Computer '\$computer\$' has been restored to Enforcement Level '\$param1\$'. |

| | Type | Subtype | ID No. | Severity | Example Descriptions/Comments |
|---|---------------------|-------------------------------------|--------|----------|---|
| Δ | Computer Management | Temporary Policy override generated | 436 | Info | User '\$username\$' has generated temporary Policy override code for computer '\$computer\$' with Enforcement Level '\$param1\$', valid for \$param2\$ minutes. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| | Computer Management | Unauthorized computer registration | 430 | Warning | An unauthorized computer registration attempt was made from \$ipaddress\$ (\$param1\$). |
| | Discovery | Banned file written to computer | 1004 | Warning | Computer \$computer\$ discovered new banned file '\$filePathAndName\$' [\$hash\$]. |
| | Discovery | Certificate added | 1013 | Info | Certificate '\$param1\$' was added by user '\$username\$'. |
| | Discovery | Certificate checked | 1014 | Info | Computer \$computer\$ reported that certificate used to sign file '\$filePathAndName\$' is invalid. Error: 0x\$param1\$ Computer \$computer\$ reported that certificate used to counter-sign file '\$filePathAndName\$' is invalid. Error: 0x\$param1\$ Server detected that certificate '\$param2\$' is invalid. Error: 0x\$param1\$ Agent detected that certificate '\$param2\$' is valid. Agent detected that certificate '\$param2\$' is invalid. Error: 0x\$param1\$ Server checked certificate '\$param2\$' for errors. Error flags: 0x\$param1\$ Agent has not been able to verify if certificate '\$param2\$' is valid. Note: "Invalid" for this event means that it has an error according to the Microsoft CryptoAPI. |
| | Discovery | Certificate revocation | 1011 | Warning | Computer \$computer\$ detected revocation of certificate '\$param2\$' on file '\$filePathAndName\$' Error: \$param1\$ Note: This event is for file-signing certificates. |
| | Discovery | Device attached | 1009 | Info | Device '\$param1\$' was attached as drive '\$param2\$'. Interactive user at the time: '\$username\$'. |
| | Discovery | Device detached | 1010 | Info | Device '\$param1\$' was detached as drive '\$param2\$'. Interactive user at the time: '\$username\$'. |
| | Discovery | External notification | 1099 | Info | \$Provider\$ reported \$notificationType\$ with name \$malwareName\$ for file \$filename\$ from \$sourceName\$[\$source_ipaddress\$] to \$destName\$[\$dest_ipaddress\$]. Found on \$num_endpoints\$ endpoints. \$Provider\$ reported no threat for file '\$filename\$'. Found on \$num_endpoints\$ endpoints. |
| ✦ | Discovery | File discovered (browser download) | 1020 | Info | The file '\$pathname\$\$pathSeparator\$\$filename\$' [\$hash\$] was downloaded by the browser \$process\$. \$param1\$ |
| ✦ | Discovery | File discovered (email attachment) | 1021 | Info | The file '\$pathname\$\$pathSeparator\$\$filename\$' [\$hash\$] was created by the email client \$process\$. \$param1\$ |
| | Discovery | File group created | 1001 | Info | Installation group was created for the file '\$filePathAndName\$' [\$hash\$]. |
| | Discovery | First execution on network | 1007 | Info | File '\$filePathAndName\$' with hash [\$hash\$] was executed for the first time. |
| | Discovery | Malicious file detected | 1201 | Critical | Unknown file '\$fileName\$' [\$hash\$] was identified by \$provider\$ as malicious. File '\$fileName\$' [\$hash\$] was identified by \$provider\$ as malicious. File '\$fileName\$' [\$hash\$] was identified by Carbon Black File Reputation as a malicious file. Note: Standard external providers are Check Point, Palo Alto Networks, or Microsoft. Other providers might be added through the App Control API. |
| | Discovery | New certificate on network | 1012 | Info | Server discovered new certificate \$SubjectName\$. Note: This event is for file-signing certificates. |
| | Discovery | New device found | 1008 | Notice | A new device '\$deviceName\$' was mounted as drive '\$drive\$'. Interactive user at the time: '\$username\$'. |

| | Type | Subtype | ID No. | Severity | Example Descriptions/Comments |
|---|--------------------|--|--------|--------------------------|---|
| | Discovery | New file on network | 1005 | Info | Server discovered new file '\$filePathAndName\$' with hash [\$hash\$]. |
| | Discovery | New publisher found | 1000 | Notice | New publisher '\$publisherName\$' was added. |
| | Discovery | New unapproved file to computer | 1003 | Notice | Computer \$computer\$ discovered new file '\$filePathAndName\$' [\$hash\$]. |
| | Discovery | Potential risk file detected | 1200 | Warning | Unknown file '\$filename\$' [\$hash\$] was identified by \$provider\$ as a potential risk File '\$filename\$' [\$hash\$] was identified by \$provider\$ as a potential risk. File '\$filename\$' [\$hash\$] was identified by Cb Reputation as a potential risk. Note: Standard external providers are Check Point, FireEye, Palo Alto Networks or Microsoft. Other providers might be added through the Carbon Black App Control API. |
| | Discovery | Service created | 1015 | Info | '\$computer\$' detected the creation of a new service: \$servicename\$. |
| | Discovery | Service deleted | 1016 | Info | '\$computer\$' detected the deletion of a service: \$servicename\$. |
| ■ | Discovery | Suspicious file found | 1022 | Info | Computer \$computer\$ detected a suspicious file '\$pathname\$\$pathSeparator\$\$filename\$' [\$hash\$]: \$param1\$ Note: This event subtype appears when App Control detects an MSI file that has data appended after the signature. |
| | General Management | Agent diagnostics available | 1117 | Info | Host '\$computer\$' generated automatic diagnostics '\$param1\$'. Note: Param1 is the name of the zip file for the diagnostic package, with timestamp in the name. |
| | General Management | Alert created | 1101 | Info | Alert '\$alertname\$' was created by '\$username\$'. |
| | General Management | Alert deleted | 1102 | Info | Alert '\$alertname\$' was deleted by '\$username\$'. |
| | General Management | Alert modified | 1103 | Info | Alert '\$alertname\$' was modified by '\$username\$'. |
| | General Management | Alert reset | 1105 | Info | Alert '\$alertname\$' was cleared by '\$username\$'. |
| | General Management | Alert triggered | 1104 | Critical /Error/ Warning | \$alertname\$: \$alertmessage\$ Examples: Revoked Certificate Alert: Certificate with subject 'New App Corp Digital ID-1' was revoked for publisher 'New App Corp' Backup Missed Alert: Scheduled database backup was not performed. Note: Previously, Notice was the severity for all alerts. Now it is: Critical for High priority alerts; Error for Medium priority alerts; Warning for Low priority alerts. |
| Δ | General Management | Baseline Drift Report created | 1106 | Info | Baseline Drift Report '\$param1\$' has been created by '\$userName\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ | General Management | Baseline Drift Report deleted | 1108 | Info | Baseline Drift Report '\$reportname1\$' has been deleted by '\$userName\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ | General Management | Baseline Drift Report generated | 1109 | Info | Baseline Drift Report '\$reportname\$' has been generated. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ | General Management | Baseline Drift Report generation is slow | 1113 | Warning | Drift report \$reportlink\$ is taking a long time to generate. You may want to consider modifying your target or setting the report size to summary only. Note: Report name is a link in this description. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ | General Management | Baseline Drift Report modified | 1107 | Info | Baseline Drift Report '\$reportname\$' has been modified by '\$userName\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |

| | Type | Subtype | ID No. | Severity | Example Descriptions/Comments |
|--------|--------------------|--------------------------------------|--------|----------|---|
| Δ | General Management | Event Rule created | 1114 | Info | Event Rule '\$ruleName\$' has been created by '\$userName\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ | General Management | Event Rule deleted | 1116 | Info | Event Rule '\$ruleName\$' has been deleted by '\$userName\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ | General Management | Event Rule modified | 1115 | Info | Event Rule '\$param1\$' has been modified by '\$userName\$'. Event Rule '\$ruleName1\$' was disabled because analysis target is no longer valid. Event Rule '\$param1\$' was disabled because file uploads are no longer allowed. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| | General Management | Meter created | 632 | Info | Meter '\$param1\$' for '\$fileName\$' was created by '\$username\$'. Note: Type was incorrectly identified as Policy Management in previous editions of this document. |
| | General Management | Meter deleted | 633 | Info | Meter '\$param1\$' for '\$fileName\$' was deleted by '\$username\$'. |
| | General Management | Meter modified | 634 | Info | Meter '\$param1\$' for '\$fileName\$' was modified by '\$username\$'. |
| ■ | General Management | Saved view cached | 1118 | Info | Saved view '\$param1\$'[id='\$param2\$'] selected for caching by user '\$username\$'. Note: This event occurs when a user requests that the current Events page view be cached. |
| ■ | General Management | Saved view cache removed | 1119 | Info | Saved view '\$param1\$'[id='\$param2\$'] removed from caching by user '\$username\$'. Note: This event occurs when a Cached Events view is removed from the Cached Events page, which also removes it from further nightly processing. |
| ■ | General Management | Saved view cache generation started | 1120 | Info | Cached view '\$param1\$' [id='\$param2\$'] generation started. Note: This event occurs when a Events page view that is queued for generation begins processing. |
| n | General Management | Saved view cache generation complete | 1121 | Info | Cached view '\$param1\$' [id='\$param2\$'] generation complete. Note: This event occurs when an Events page view queued for caching has been processed and is available on the Cached Events page in the console. |
| | General Management | Snapshot created | 1110 | Info | Snapshot '\$snapshotName\$' has been created by '\$userName\$'. |
| | General Management | Snapshot deleted | 1112 | Info | Snapshot '\$ snapshotName \$' has been deleted by '\$userName\$'. |
| | General Management | Snapshot modified | 1111 | Info | Snapshot '\$ snapshotName \$' has been modified by '\$userName\$'. |
| Δ | Policy Enforcement | Access block (Memory Rule) | 830 | Notice | Access to process '\$filePathAndName\$' was restricted - Requested[\$param1\$] Restricted[\$param2\$]. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ | Policy Enforcement | Access prompt (Memory Rule) | 831 | Info | Access to process '\$filePathAndName\$' was granted because of a Memory Rule user response. Access to process '\$filePathAndName\$' was restricted because of a Memory Rule user response. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ Ⓜ | Policy Enforcement | Banned process discovered | 847 | Warning | The Carbon Black App Control Agent discovered a banned process '\$pathname\$\$pathSeparator\$\$filename\$' [\$hash\$] that ran during system startup. \$param1\$ Change Note: Capitalization of the subtype was changed in v8.1.0. Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0. |
| ◇ Ⓜ | Policy Enforcement | Carbon Black EDR Watchlist | 842 | Notice | If Process watchlist and file are known to App Control: Carbon Black EDR process watchlist '\$ruleName\$' hit for process '\$process\$' [\$hash\$] on computer '\$computer\$'. Carbon Black EDR watchlist '\$watchlist\$' detected file '\$filePathAndName\$' [\$hash\$] on computer '\$computer\$'. If Process watchlist and file are unknown to App Control: |

| | Type | Subtype | ID No. | Severity | Example Descriptions/Comments |
|---|--------------------|---|--------|----------|---|
| | | | | | <p>Carbon Black EDR process watchlist '\$ruleName\$' hit for unknown process '\$process\$' [\$processhash\$] on computer '\$computer\$'.</p> <p>Carbon Black EDR watchlist '\$watchlist\$' detected unknown file '\$filePathAndName\$' [\$hash\$] on computer '\$computer\$'.</p> <p>(continued on next page)</p> <p>(continued from previous page)</p> <p>If Binary watchlist and file are known to App Control:</p> <p>Carbon Black EDR binary watchlist '\$ruleName\$' detected file '\$filePathAndName\$' [\$hash\$].</p> <p>If Binary watchlist and file is unknown to App Control:</p> <p>Carbon Black EDR binary watchlist '\$ruleName\$' detected unknown file '\$filePathAndName\$' [\$hash\$].</p> <p>Change Note: Prior to v8.0.0, "Carbon Black EDR" in the subtype and descriptions was "Carbon Black". Capitalization of the subtype changed in v8.1.0.</p> <p>Change Note: CB Response replaced with Carbon Black EDR in v8.5.0.</p> |
| O | Policy Enforcement | Execution allowed (file loaded before kernel) | 843 | Warning | <p>The \$param1\$ file '\$pathname\$\$pathSeparator\$\$filename\$' [\$hash\$] executed before the Carbon Black App Control Agent was running. \$param2\$</p> <p>Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0.</p> |
| Ⓜ | Policy Enforcement | Execution allowed (file loaded before service) | 844 | Warning | <p>The \$param1\$ file '\$pathname\$\$pathSeparator\$\$filename\$' [\$hash\$] executed before the Carbon Black App Control Agent was enforcing. \$param2\$</p> <p>Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0.</p> |
| Ⓜ | Policy Enforcement | Execution allowed (inactive) | 841 | Warning | <p>Execution of file '\$filePathAndName\$' [\$hash\$] would have blocked if Carbon Black App Control Agent was active.</p> <p>Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0.</p> |
| Δ | Policy Enforcement | Execution allowed (Trusted User) | 815 | Notice | <p>Execution of unapproved file '\$filePathAndName\$' [\$hash\$] was allowed because of a Trusted User '\$username\$'.</p> <p>Change Note: Capitalization of the subtype was changed in v8.1.0.</p> |
| Ⓜ | Policy Enforcement | Execution allowed (Unanalyzed file loaded before service) | 846 | Warning | <p>The file '\$pathname\$\$pathSeparator\$\$filename\$' executed before the Carbon Black App Control Agent started. The file was removed before the Carbon Black App Control Agent could analyze it. \$param2\$</p> <p>Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0.</p> |
| | Policy Enforcement | Execution block (banned file) | 802 | Notice | <p>File '\$filePathAndName\$' [\$hash\$] was blocked because it was banned.</p> |
| Δ | Policy Enforcement | Execution block (Custom Rule) | 806 | Notice | <p>File '\$filePathAndName\$' with hash [\$hash\$] was blocked because of a Custom Rule. Process '\$process\$' was terminated due to a Custom Rule.</p> <p>Change Note: Capitalization of the subtype was changed in v8.1.0.</p> |
| | Policy Enforcement | Execution block (network file) | 805 | Notice | <p>The file '\$filePathAndName\$' [\$hash\$] was blocked because it was located on a remote drive.</p> |
| | Policy Enforcement | Execution block (prompt timeout) | 839 | Info | <p>File '\$filePathAndName\$' with hash [\$hash\$] was blocked because of a timeout waiting for user response.</p> |
| | Policy Enforcement | Execution block (removable media) | 819 | Notice | <p>File '\$filePathAndName\$' with hash [\$hash\$] was blocked from execution because it was on removable media.</p> |
| Ⓜ | Policy Enforcement | Execution block (still analyzing) | 804 | Info | <p>File '\$filePathAndName\$' was blocked because Carbon Black App Control Agent did not have time to analyze it.</p> <p>Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0.</p> |

| | Type | Subtype | ID No. | Severity | Example Descriptions/Comments |
|--------|---------------------------|--|--------|----------|---|
| | Policy Enforcement | Execution block (unapproved file) | 801 | Notice | File '\$filePathAndName\$' [\$hash\$] was blocked because it was unapproved. |
| Δ | Policy Enforcement | Execution prompt (Custom Rule) | 818 | Info | File '\$filePathAndName\$' [\$hash\$] was executed because of a Custom Rule user response. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| | Policy Enforcement | Execution prompt (unapproved file) | 814 | Info | File '\$filePathAndName\$' [\$hash\$] was approved because of a user response. |
| | Policy Enforcement | Execution prompt allowed (unapproved file) | 838 | Info | File '\$filePathAndName\$' [\$hash\$] was approved because of a user response. |
| | Policy Enforcement | Execution prompt block (unapproved file) | 837 | Info | File '\$filePathAndName\$' [\$hash\$] was blocked because of a user response. |
| | Policy Enforcement | File access error | 825 | Warning | Unable to access the file '\$filePathAndName\$'. |
| | Policy Enforcement | File approved (cache consistency) | 835 | Info | File '\$filePathAndName\$' [\$hash\$] was approved due to cache a consistency scan. |
| Δ | Policy Enforcement | File approved (Custom Rule) | 833 | Info | File '\$filePathAndName\$' [\$hash\$] was approved due to Custom Rule. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| | Policy Enforcement | File approved (local approval) | 813 | Info | File '\$filePathAndName\$' [\$hash\$] was locally approved. |
| | Policy Enforcement | File approved (publisher) | 812 | Info | File '\$filePathAndName\$' [\$hash\$] was approved by Publisher '\$publisherName\$'. |
| Δ | Policy Enforcement | File approved (Reputation) | 840 | Info | File '\$filePathAndName\$' [\$hash\$] was approved by reputation. Note: This event occurs when an agent attempts to run an unapproved file, checks with the server, and is given a reputation approval from the server that was not previously sent to the agent. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| | Policy Enforcement | File approved (system update) | 836 | Info | File '\$filePathAndName\$' with hash [\$hash\$] was approved due to system update. Note: For Windows, this applies to the package/root files from Windows Update, not files installed from them. |
| Δ | Policy Enforcement | File approved (Trusted User) | 810 | Info | File '\$filePathAndName\$' [\$hash\$] was approved by Trusted User '\$username\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| ✦ | Policy Enforcement | File approved (Unidesk) | 850 | Info | The file '\$pathname\$\$pathSeparator\$\$filename\$' [\$hash\$] was approved due to Unidesk read-only provisioning. '\$param1\$' '\$param2\$' |
| | Policy Enforcement | File approved (updater) | 811 | Info | File '\$filePathAndName\$' [\$hash\$] was approved by an Updater. |
| | Policy Enforcement | File approved (version resource) | 834 | Info | File '\$filePathAndName\$' [\$hash\$] was approved due to version resource. |
| ■ | Policy Enforcement | File approved (Yara) | 852 | Info | The file '\$pathname\$\$pathSeparator\$\$filename\$' [\$hash\$] was approved due to yara rule(s). '\$param1\$' '\$param2\$' |
| | Policy Enforcement | Metered execution | 816 | Notice | Metered file '\$filePathAndName\$' [\$hash\$] was executed by the user '\$username\$'. |
| ◇ 📁 | Policy Enforcement | New file discovered on startup | 845 | Warning | The newly discovered file '\$pathname\$\$pathSeparator\$\$filename\$' [\$hash\$] was executing when the Carbon Black App Control Agent started. '\$param1\$' Change Note: Prior to v8.0.0, the subtype was "Execution allowed (New file discovered on startup)". Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0. |
| | Policy Enforcement | Prompt canceled | 849 | Warning | Prompt '\$filePathAndName\$' [\$hash\$] prompt is canceled ('\$param1\$'). Note: Param1 shows the reason a notifier prompt was cancelled. It can be one of the following: <ul style="list-style-type: none"> EnforcementChange – Agent changed enforcement levels and the prompt no longer applies (e.g., moved from Medium to High, so the file will now just block). |

| | Type | Subtype | ID No. | Severity | Example Descriptions/Comments |
|--------|--------------------|------------------------------------|--------|----------|--|
| | | | | | <ul style="list-style-type: none"> • <i>SubsequentBlock</i> – Agent blocked the file and is no longer waiting for response (typically means timeout or file was banned or had a rule change the blocked it). • <i>AgentShutdown</i> – System or daemon shutdown while the prompt was still outstanding. File will be blocked in this case. • <i>PingTimeout</i> – Agent was unable to communicate with notifier and canceled the prompt. This is an error case and should be rare. <p>Platform Note: This event only occurs for Mac OS X and Linux agents.</p> |
| | Policy Enforcement | Read block (removable media) | 821 | Notice | Read access to file '\$filePathAndName\$' with hash [\$hash\$] was blocked because it was on removable media. |
| Δ | Policy Enforcement | Report access (Memory Rule) | 829 | Info | Access to process '\$filePathAndName\$' was granted – Requested[\$param1\$] Note: Param1 is a hex number indicating the Windows code of the permissions requested. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ | Policy Enforcement | Report execution (Custom Rule) | 807 | Notice | File '\$filePathAndName\$' [\$hash\$] was executed. Process '\$process\$' failed to be terminated: \$param3\$. Banned image: '\$filePathAndName\$' [\$hash\$]. Process '\$process\$' would have been terminated due to the banned file '\$filePathAndName\$' [\$hash\$] if Policy were not in Visibility Only Process '\$process\$' would have been terminated due to the banned image '\$filePathAndName\$' [\$hash\$]: \$param3\$." Change Note: Capitalization of the subtype was changed in v8.1.0. |
| | Policy Enforcement | Report execution (removable media) | 822 | Info | File '\$filePathAndName\$' with hash [\$hash\$] was executed on removable media. |
| | Policy Enforcement | Report execution block | 803 | Notice | File '\$filePathAndName\$' [\$hash\$] would have blocked if a ban were not in Report Only mode. |
| | Policy Enforcement | Report read (removable media) | 824 | Info | File '\$filePathAndName\$' was read on removable media. |
| Δ | Policy Enforcement | Report write (Custom Rule) | 809 | Info | File '\$filePathAndName\$' was modified or deleted. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ ◇ | Policy Enforcement | Report write (Registry Rule) | 826 | Info | Modification of registry '\$filePathAndName\$' was allowed. Change Note: The wording of the Description was modified slightly in v8.0.0. Subtype capitalization changed in v8.1.0. |
| | Policy Enforcement | Report write (removable media) | 823 | Info | File '\$filePathAndName\$' was modified or deleted on removable media. |
| D | Policy Enforcement | Tamper Protection | 832 | Warning | Execution of '\$filePathAndName\$' by '\$username\$' was blocked because tamper protection was enabled. Modification of '\$filePathAndName\$' by '\$username\$' was blocked because tamper protection was enabled. Execution of '\$filePathAndName\$' by '\$username\$' would have been blocked if tamper protection were enabled. Modification of '\$filePathAndName\$' by '\$username\$' would have been blocked if tamper protection were enabled. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ ⌘ | Policy Enforcement | Unapproved process discovered | 848 | Warning | The Carbon Black App Control Agent discovered an unapproved process '\$filePathAndName\$' [\$hash\$] that ran during system startup. \$param1\$ Change Note: Capitalization of the subtype was changed in v8.1.0. |

| | Type | Subtype | ID No. | Severity | Example Descriptions/Comments |
|--------|--------------------|------------------------------------|--------|----------|---|
| | | | | | Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0. |
| ⊙ | Policy Enforcement | User Login denied | 853 | Warning | User '\$param1\$' prohibited from logging in on computer \$computer\$. |
| Δ | Policy Enforcement | Write block (Custom Rule) | 808 | Notice | Modification of file '\$filePathAndName\$' [\$hash\$] was blocked because of a Custom Rule. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ | Policy Enforcement | Write block (Registry Rule) | 827 | Notice | Modification of registry '\$filePathAndName\$' was blocked. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| | Policy Enforcement | Write block (removable media) | 820 | Notice | Modification of file '\$filePathAndName\$' with hash [\$hash\$] was blocked because it was on removable media. |
| Δ | Policy Enforcement | Write prompt (Custom Rule) | 817 | Info | File '\$filePathAndName\$' was modified or deleted because of a Custom Rule user response. Modification of file '\$filePathAndName\$' [\$hash\$] was blocked because of a Custom Rule user response. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ | Policy Enforcement | Write prompt (Registry Rule) | 828 | Info | Registry '\$filePathAndName\$' was modified or deleted because of a Registry Rule user response. Modification of registry '\$filePathAndName\$' was blocked because of a Registry Rule user response. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| | Policy Management | AD rules loaded | 605 | Info | Active Directory rules script with version \$param1\$ was loaded successfully. |
| Δ ◇ | Policy Management | Approval Request closed | 646 | Info | Approval Request Id \$requestID\$ was closed by user '\$username\$' as '\$resolvedState\$' with '\$comment\$'. Change Note: The request ID was added to the Description field in v8.0.0. Subtype capitalization changed in v8.1.0. |
| Δ ◇ | Policy Management | Approval Request created | 644 | Info | Approval Request Id \$requestID\$ was created by user '\$username\$'. Change Note: The request ID was added to the Description field in v8.0.0. Subtype capitalization changed in v8.1.0. |
| Δ + | Policy Management | Approval Request duplicate created | 661 | Info | Duplicate of Approval Request Id \$requestID\$ was created by user '\$username\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ + | Policy Management | Approval Request escalated | 663 | Info | Approval Request Id \$requestID\$ was escalated by user '\$username\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ + | Policy Management | Approval Request modified | 662 | Info | Approval Request Id \$requestID\$ was modified by user '\$username\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ ◇ | Policy Management | Approval Request opened | 645 | Info | Approval Request Id \$requestID\$ was opened by user '\$username\$'. Change Note: The request ID was added to the Description field in v8.0.0. Subtype capitalization changed in v8.1.0. |
| | Policy Management | Certificate approval created | 651 | Info | Certificate \$SubjectName\$ was approved by '\$username\$' for publisher \$publisher\$. |
| | Policy Management | Certificate approval deleted | 653 | Info | Approval of certificate \$SubjectName\$ was deleted by '\$username\$' for publisher \$publisher\$. |
| | Policy Management | Certificate approval modified | 652 | Info | Approval of certificate '\$param1\$' was modified by '\$username\$' for publisher '\$param3\$'. |
| | Policy Management | Certificate ban created | 654 | Info | Certificate \$SubjectName\$ was banned by \$username\$ for publisher \$publisher\$. |
| | Policy Management | Certificate ban deleted | 656 | Info | Ban of certificate \$SubjectName\$ was deleted by '\$username\$' for publisher \$publisher\$. |
| | Policy Management | Certificate ban modified | 655 | Info | Ban of certificate '\$subjectName\$' was modified by '\$username\$' for publisher '\$param3\$'. |

| | Type | Subtype | ID No. | Severity | Example Descriptions/Comments |
|--------|-------------------|-----------------------------|--------|----------|---|
| △ ◇ | Policy Management | Custom Rule created | 638 | Info | Custom Rule '\$ruleName\$' was created by '\$username\$'. Custom Rule '\$ruleName\$ (Unified)' was created by '\$username\$'. '\$ruleName\$' was imported by '\$username\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| △ ◇ | Policy Management | Custom Rule deleted | 640 | Info | Custom Rule '\$ruleName\$' was deleted by '\$username\$'. Custom Rule '\$ruleName\$ (Unified)' was deleted by '\$username\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| △ ◇ | Policy Management | Custom Rule modified | 639 | Info | Custom Rule '\$ruleName\$' was modified by '\$username\$'. Custom Rule '\$ruleName\$ (Unified)' was modified by '\$username\$'. '\$ruleName\$' was imported by '\$username\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| △ | Policy Management | Device Rule created | 641 | Info | Device Rule for '\$ruleName\$' with id '\$ruleID\$' was created by '\$username\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| △ | Policy Management | Device Rule deleted | 642 | Info | Rule for device '\$deviceName\$' with id '\$ruleID\$' was removed by '\$username\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| △ | Policy Management | Device Rule modified | 643 | Info | Device Rule '\$ruleName\$' with id '\$ruleID\$' was modified by '\$username\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| ◇ | Policy Management | File approval created | 627 | Info | Approval '\$ruleName\$' for hash [\$hash\$] was created by '\$username\$'. Approval '\$ruleName (Unified)' for hash [\$hash\$] was created by '\$username\$'. File '\$filePath\$ ' with hash [\$hash\$] was approved based on Reputation. \$param1\$ files were approved based on Reputation. Notes: This event occurs when the rule is created on the server, not when a file instance is approved. In the last example, '\$param1\$ files' links to a list of files approved by reputation in this event. |
| ◇ | Policy Management | File approval deleted | 629 | Info | Approval '\$ruleName\$' for hash [\$hash\$] was deleted by '\$username\$'. Approval '\$ruleName (Unified)' for hash [\$hash\$] was deleted by '\$username\$'. Approval of file '\$pathname\$\$pathSeparator\$\$filename\$' with hash [\$hash\$] was removed based on Reputation. Approval of \$param1\$ files were removed based on Reputation. Notes: This event occurs when the approval rule is deleted on the server, not when approval of a file instance is removed. For the last example, '\$param1\$ files' is a link to the Files on Computers page where the files whose approvals were removed will be listed if they still exist in their respective locations. |
| | Policy Management | File approval modified | 628 | Info | Approval '\$ruleName\$' for hash [\$hash\$] was modified by '\$username\$'. Approval '\$ruleName (Unified)' for hash [\$hash\$] was modified by '\$username\$'. |
| | Policy Management | File approved (certificate) | 660 | Info | File '\$filePathAndName\$' was approved by certificate '\$param1\$'. |
| ◇ | Policy Management | File ban created | 635 | Info | Ban '\$name\$' for [\$hash\$] was created by '\$username\$'. Ban '\$name\$ (Unified)' for [\$hash\$] was created by '\$username\$'. Note: \$name\$ is either the name of the banned file or a user-created name (usually for multi-file bans). |
| ◇ | Policy Management | File ban deleted | 637 | Info | Ban '\$name\$' for [\$hash\$] was deleted by '\$username\$'. Ban '\$name\$ (Unified)' for [\$hash\$] was deleted by '\$username\$'. |

| | Type | Subtype | ID No. | Severity | Example Descriptions/Comments |
|--------|-------------------|------------------------------------|--------|----------|---|
| | | | | | Note: \$name\$ is the name of the banned file or a user-created name (usually for multi-file bans). |
| ◇ | Policy Management | File ban modified | 636 | Info | Ban '\$name\$' for [\$hash\$] was modified by '\$username\$'. Ban '\$name\$ (Unified)' for [\$hash\$] was modified by '\$username\$'. Note: \$name\$ is the name of the banned file or a user-created name (usually for multi-file bans). |
| | Policy Management | File local approval | 623 | Info | File '\$filePathAndName\$' [\$hash\$] was locally approved on computer \$computer\$ by '\$userName\$'. |
| | Policy Management | File properties modified | 611 | Info | There are multiple possible descriptions for this subtype. Examples: File [\$hash\$] was approved by '\$username\$'. File [\$hash\$] was marked as an installer by '\$username\$'. Reputation was disabled for file [\$hash\$] by '\$username\$'. |
| | Policy Management | File remove local approval | 625 | Info | File '\$filePathAndName\$' [\$hash\$] was changed to unapproved on computer \$computer\$ by '\$userName\$'. |
| ○ | Policy Management | Install package creation scheduled | 603 | Notice | An \$param1\$ install package \$policyName\$.msi was scheduled for creation by '\$username\$'. Note: Param1 is either empty or "automatic" for packages that allow automatic AD Policy assignment. Change Note: The subtype and description were changed in v8.1.4 to indicate that the installation is scheduled, not completed. |
| △ | Policy Management | Justification created | 650 | Info | Justification Id \$param2\$ was created by user '\$username\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| ✦ | Policy Management | Justification duplicate created | 664 | Info | Duplicate of Justification Id \$param2\$ was created by user '\$username\$'. |
| △ ◇ | Policy Management | Memory Rule created | 129 | Info | Memory Rule '\$ruleName\$' created by '\$username\$'. Memory Rule '\$ruleName\$ (Unified)' created by '\$username\$'. '\$ruleName\$' was imported by '\$username\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| D ◇ | Policy Management | Memory Rule deleted | 131 | Info | Memory Rule '\$ruleName\$' deleted by '\$username\$'. Memory Rule '\$ruleName\$ (Unified)' deleted by '\$username\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| △ ◇ | Policy Management | Memory Rule modified | 130 | Info | Memory Rule '\$ruleName\$' modified by '\$username\$'. Memory Rule '\$ruleName\$ (Unified)' modified by '\$username\$'. '\$ruleName\$' was imported by '\$username\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| | Policy Management | Notifier created | 153 | Info | Notifier '\$notifierName\$' was created by '\$username\$' |
| | Policy Management | Notifier deleted | 154 | Info | Notifier '\$notifierName\$' was deleted by '\$username\$' |
| | Policy Management | Notifier modified | 155 | Info | Notifier '\$notifierName\$' was modified by '\$username\$' |
| ◇ | Policy Management | Policy AD rules changed | 604 | Notice | '\$username\$' created an AD rule for mapping \$param1\$ to the Policy \$policyName\$. Change Note: Prior to v8.0.0, the event subtype was "AD Rules changed". The type was changed because there are now mapping rules for user login accounts. |
| | Policy Management | Policy created | 600 | Info | Policy '\$policyName\$' was created by '\$username\$'. |
| | Policy Management | Policy deleted | 601 | Info | Policy '\$policyName\$' was deleted by '\$username\$'. |
| | Policy Management | Policy file tracking disabled | 606 | Notice | File tracking has been disabled for Policy '\$policyName\$' by '\$userName\$'. |

| | Type | Subtype | ID No. | Severity | Example Descriptions/Comments |
|--------|-------------------|------------------------------|--------|----------|--|
| | Policy Management | Policy file tracking enabled | 607 | Notice | File tracking has been enabled for Policy '\$policyName\$' by '\$userName\$'. |
| | Policy Management | Policy modified | 602 | Info | Policy '\$policyName\$' was modified by '\$userName\$'. |
| | Policy Management | Process demoted | 1006 | Notice | Process \$filePathAndName\$ was demoted on the computer '\$computer\$'. New files written by this process will be unapproved. |
| | Policy Management | Publisher approval created | 618 | Info | Publisher '\$publisherName\$' was approved by '\$userName\$'. |
| | Policy Management | Publisher approval removed | 619 | Info | Publisher '\$publisherName\$' approval was removed by '\$userName\$'. |
| | Policy Management | Publisher ban created | 657 | Info | Publisher '\$publisherName\$' was banned by '\$userName\$'. |
| | Policy Management | Publisher ban deleted | 659 | Info | Publisher '\$publisherName\$' ban was removed by '\$userName\$'. |
| | Policy Management | Publisher modified | 630 | Info | Publisher '\$publisherName\$' was edited by '\$userName\$'. |
| Δ ◇ | Policy Management | Registry Rule created | 132 | Info | Registry Rule '\$ruleName\$' created by '\$userName\$'. Registry Rule '\$ruleName\$ (Unified)' created by '\$userName\$'. '\$ruleName\$' was imported by '\$userName\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ ◇ | Policy Management | Registry Rule deleted | 134 | Info | Registry Rule '\$ruleName\$' deleted by '\$userName\$'. Registry Rule '\$ruleName\$ (Unified)' deleted by '\$userName\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ ◇ | Policy Management | Registry Rule modified | 133 | Info | Registry Rule '\$ruleName\$' modified by '\$userName\$'. Registry Rule '\$ruleName\$ (Unified)' modified by '\$userName\$'. '\$ruleName\$' was imported by '\$userName\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| | Policy Management | Reputation settings modified | 144 | Info | Reputation was enabled by '\$userName\$'. Reputation was disabled by '\$userName\$'. Reputation settings were modified by '\$userName\$'. |
| | Policy Management | Rules exported | 200 | Info | Custom Rules were exported by '\$userName\$'. Memory Rules were exported by '\$userName\$'. Registry Rules were exported by '\$userName\$'. |
| Δ | Policy Management | Script Rule created | 647 | Info | Script Rule '\$ruleName\$' was created by '\$userName\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ | Policy Management | Script Rule deleted | 648 | Info | Script Rule '\$ruleName\$' was deleted by '\$userName\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ | Policy Management | Script Rule modified | 649 | Info | Script Rule '\$ruleName\$' was modified by '\$userName\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ | Policy Management | Trusted Directory check | 608 | Info | Trusted Directory '\$pathName\$' on computer '\$computer\$' is '\$param2\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ | Policy Management | Trusted Directory created | 613 | Info | Approval directory '\$pathname\$' added by '\$userName\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ | Policy Management | Trusted Directory deleted | 615 | Info | Approval directory '\$pathname\$' deleted by '\$userName\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |

| | Type | Subtype | ID No. | Severity | Example Descriptions/Comments |
|---|-------------------|--|--------|----------------------|--|
| Δ | Policy Management | Trusted Directory import | 626 | Info, Warning, Error | Trusted package '\$param1\$' from '\$source\$' has been processed. Notes: Source may be a computer name or a manifest name. Severity is Info for status imports; Warning for improperly signed or misidentified manifests; Error for all other cases. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ | Policy Management | Trusted Directory modified | 614 | Info | Approval directory '\$filePathAndName\$' modified by '\$username\$'. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ | Policy Management | Trusted Directory scan | 609 | Info | Pre-approval scan started for '\$filePathAndName\$'. Approval ID: \$param1\$. Job ID: \$param2\$. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| | Policy Management | Trusted User added | 616 | Info | Trusted User '\$name\$' was added by '\$consoleusername\$'. |
| | Policy Management | Trusted User deleted | 617 | Info | Trusted User '\$name\$' was deleted by '\$consoleusername\$'. |
| ✦ | Policy Management | Unified rule overridden | 665 | Info | Unified rule '\$param1\$' was overridden by '\$username\$' Note: In the initial release of v8.0.0, "overridden" was misspelled in the subtype and description. |
| | Policy Management | Updater disabled | 621 | Info | Updater '\$updaterName\$' was disabled by '\$username\$'. |
| | Policy Management | Updater enabled | 620 | Info | Updater '\$updaterName\$' was enabled by '\$username\$'. |
| ■ | Policy Management | Yara rule created | 220 | Info | Yara Rule '\$param1\$' created by '\$username\$'. |
| ■ | Policy Management | Yara rule deleted | 222 | Info | Yara Rule '\$param1\$' deleted by '\$username\$'. |
| ■ | Policy Management | Yara rule modified | 221 | Info | Yara Rule '\$param1\$' modified by '\$username\$'. |
| | Server Management | AD lookups are slow | 114 | Warning | Active Directory Lookups are slow. Average lookup took \$param1\$ ms. Please review your AD configuration. |
| ● | Server Management | Agent install package generation disabled | 214 | Error | Agent install package generation is disabled for all operating systems. To enable agent generation, please download rules and host packages from the Carbon Black User eXchange at https://community.carbonblack.com/ . |
| | Server Management | Agent install package generation failed | 231 | Error | \$platform\$ agent install packages failed to generate for policy '\$policy\$' |
| ● | Server Management | Agent install package generation succeeded | 213 | Info | \$platform\$ agent install packages have been successfully generated. |
| | Server Management | Agent SSL error | 126 | Warning | SSL certificate error was detected when talking with host at IP '\$ipAddress\$'. This event can be falsely triggered by unreliable network connections. Change Notes: Subtype was "Agent certificate expired" in some previous versions. |
| ◇ | Server Management | Carbon Black File Reputation connection lost | 138 | Warning | Carbon Black File Reputation connection lost: \$reason\$ Change Note: In pre-8.0.0 releases, the subtype referred to "Parity Knowledge Service" or "Bit9 Software Reputation Service." |
| ◇ | Server Management | Carbon Black File Reputation connection restored | 139 | Notice | Carbon Black File Reputation connection restored Change Note: In pre-8.0.0 releases, the subtype referred to "Parity Knowledge Service" or "Bit9 Software Reputation Service." |
| ◇ | Server Management | Carbon Black File Reputation proxy cleared | 141 | Info | Proxy disabled. Using direct connection to Carbon Black File Reputation. Change Note: In pre-8.0.0 releases, the subtype referred to "Parity Knowledge Service" or "Bit9 Software Reputation Service." |

| | Type | Subtype | ID No. | Severity | Example Descriptions/Comments |
|---|-------------------|---|--------|-----------------|---|
| ◇ | Server Management | Carbon Black File Reputation proxy set | 140 | Info | Using proxy '\$param1\$' for connection to Carbon Black File Reputation. Change Note: In pre-8.0.0 releases, the subtype referred to "Parity Knowledge Service" or "Bit9 Software Reputation Service." |
| | Server Management | Communication error | 136 | Error | SOAP error on computer \$computer\$ (\$ipaddress\$) in \$param1\$. |
| | Server Management | Connector restart | 178 | Warning | Connector started, build information: \$param1\$ |
| | Server Management | Connector shutdown | 179 | Notice | Connector shutdown cleanly. |
| | Server Management | Database error | 135 | Error | Unknown error initializing database pool. |
| | Server Management | Database server reached specified limit | 106 | Critical | Database data file size limit reached. Total data file size is \$param1\$ MB. |
| Ⓜ | Server Management | Database verification error | 108 | Error | Carbon Black App Control Server database is corrupt: \$param1\$. Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0. |
| ● | Server Management | Default rules not found | 230 | Error | Failed to generate agent install packages because the default rules do not exist. To enable agent generation, please download rules from the Carbon Black User eXchange at https://community.carbonblack.com/ . |
| | Server Management | Enabled Indicator Set deleted | 169 | Info | Indicator Set \$setName\$ was deleted by '\$username\$' Note: Occurs only when the Indicator Set was enabled at the time of deletion. There is a different Indicator Set deleted event for the general case. |
| | Server Management | Enabled updater deleted | 148 | Info | Enabled Updater \$updaterName\$ was deleted by '\$username\$' Note: Occurs only when the Updater was enabled at the time of deletion. |
| | Server Management | File analysis canceled | 158 | Info | User '\$username\$' canceled analysis of file '\$filename\$' [\$hash\$] with '\$provider\$'. |
| | Server Management | File analysis completed | 161 | Info Warning | File '\$filename\$' [\$hash\$] was successfully analyzed with '\$provider\$'. Nothing suspicious was found. File '\$filename\$' [\$hash\$] was successfully analyzed with '\$provider\$'. It was reported as malicious. |
| | Server Management | File analysis error | 160 | Error | Analysis of file '\$filename\$' [\$hash\$] with '\$provider\$' failed because of error '\$param1\$'. |
| | Server Management | File analysis modified | 176 | Info | 'User "\$username\$" modified priority of analysis of file [\$hash\$]. |
| | Server Management | File analysis requested | 157 | Info | User '\$username\$' requested analysis of file [\$hash\$] with '\$provider\$'. Analysis of file [\$hash\$] with '\$provider\$' was requested by Event Rule '\$ruleName\$'. |
| ★ | Server Management | File downloaded | 196 | Info | File '\$filename\$' [\$hash\$] downloaded by '\$username\$' from server |
| | Server Management | File inventory deleted | 187 | Notice | Deleted \$param1\$ inventory files that were excluded per configuration Note: Param1 is the number of files deleted. |
| | Server Management | File tracking disabled | 109 | Warning | File tracking has been automatically disabled because database data file size limit has been reached. |
| | Server Management | File upload modified | 177 | Info | User '\$username\$' modified priority of upload of file [\$hash\$] from computer '\$computer\$' |
| Δ | Server Management | Health Indicator changed | 183 | Info | The System has changed Health Indicator '\$Param1\$' on tab '\$Param2\$' on the System Health page. Notes: Param1 is the name of the Health Indicator. Param2 is the tab on which it appears. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ | Server Management | Health Indicator created | 182 | Info | A new Health Indicator '\$Param1\$' was created by \$username\$ on the '\$Param2\$' tab of the System Health page. Note: Param1 is the name of the Health Indicator. Param2 is the tab on which it appears. |

| | Type | Subtype | ID No. | Severity | Example Descriptions/Comments |
|---|-------------------|----------------------------------|--------|---------------|---|
| | | | | | Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ | Server Management | Health Indicator deleted | 184 | Info | The system has removed Health Indicator '\$Param1\$' from tab '\$Param2\$' on the System Health Page. Note: Param1 is the name of the Health Indicator. Param2 is the tab where it previously appeared. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ | Server Management | Health Indicator severity change | 181 | Warning /Info | For existing Health Indicators: Health Indicator '\$Param1\$' has changed from severity '\$Param2\$' to severity '\$Param3\$'. Health Indicator '\$Param1\$' has gone to severity Param3\$. Check the Health Indicator for more details. (Appears when indicator stops showing healthy state) Health Indicator '\$Param1\$' has increased in severity from '\$Param2\$' to '\$Param3\$'. Check the Health Indicator for more details. (Appears when indicator moves from borderline to critical) Health Indicator '\$Param1\$' has decreased in severity from Param2\$ to Param3\$. (Appears when indicator moves from critical to borderline) Health Indicator '\$Param1\$' is now healthy. (Appears when indicator moves to healthy state) For newly created Health Indicators: Newly created Health Indicator '\$Param1\$' is healthy. Newly created Health Indicator '\$Param1\$' has severity '\$Param3\$'. Check the Health Indicator for more details. Change Note: Capitalization of the subtype was changed in v8.1.0. |
| ● | Server Management | Host package not found (Linux) | 217 | Error | Failed to generate agent install packages for Linux because the host package does not exist. To enable agent generation, please download host packages from the Carbon Black User eXchange at https://community.carbonblack.com/ . |
| ● | Server Management | Host package not found (Mac) | 216 | Error | Failed to generate agent install packages for Mac because the host package does not exist. To enable agent generation, please download host packages from the Carbon Black User eXchange at https://community.carbonblack.com/ . |
| ● | Server Management | Host package not found (Windows) | 215 | Error | Failed to generate agent install packages for Windows because the host package does not exist. To enable agent generation, please download host packages from the Carbon Black User eXchange at https://community.carbonblack.com/ . |
| | Server Management | Indicator Set created | 163 | Info | Indicator Set '\$setName\$' was created by '\$username\$'. |
| | Server Management | Indicator Set deleted | 164 | Info | Indicator Set '\$setName\$' was deleted by '\$username\$' Note: There is a separate Enabled Indicator Set deleted event for Updaters deleted while enabled. |
| | Server Management | Indicator Set disabled | 167 | Info | Indicator Set '\$setName\$' was disabled by '\$username\$' |
| | Server Management | Indicator Set enabled | 166 | Info | Indicator Set '\$setName\$' was enabled by '\$username\$' |
| | Server Management | Indicator Set exception created | 172 | Info | Indicator Set Exception '\$setName\$' created by '\$username\$' |
| | Server Management | Indicator Set exception deleted | 174 | Info | Indicator Set Exception '\$param1\$' deleted by '\$username\$' |
| | Server Management | Indicator Set exception modified | 173 | Info | Indicator Set Exception '\$param1\$' modified by '\$username\$' |
| | Server Management | Indicator Set modified | 168 | Info | Indicator Set '\$param1\$' was modified by '\$username\$' |
| | Server Management | Indicator Set updated | 165 | Info | Indicator Set '\$param1\$' was updated by '\$username\$' |
| ● | Server Management | Install failed | 212 | Error | "\$param1\$ install failed. \$param2\$" Note: \$param1\$ is the installation file for the agent host package or default rules file and \$param2\$ is the reason for the failure, such as failed signature verification. |

| | Type | Subtype | ID No. | Severity | Example Descriptions/Comments |
|---|-------------------|---------------------------|--------|----------|---|
| ● | Server Management | Install succeeded | 211 | Info | \$param1\$ install successful Note: \$param1\$ specifies a host package platform and version or a default rules version. |
| Ⓜ | Server Management | License added | 115 | Notice | User '\$username\$' has successfully added new Carbon Black App Control license. Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0. |
| O | Server Management | License error | 116 | Error | User '\$username\$' attempted to add Carbon Black App Control license. (\$param1\$) Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0. |
| Ⓜ | Server Management | License warning | 117 | Warning | Your Carbon Black App Control Suite license will expire in \$param1\$ day(s) on \$date\$. Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0. |
| | Server Management | Network Connector | 162 | Info | New network connector '\$product\$', version '\$param2\$' was registered. Network connector '\$product\$', version '\$param2\$' was removed. Network connector '\$product\$', version '\$param2\$' was removed and its data was deleted. User '\$username\$' has modified configuration of network connector '\$product\$'. User '\$user\$' has modified UI configuration of network connector '\$param1\$'. User '\$username\$' has enabled network connector '\$product\$'. User '\$username\$' has disabled network connector '\$product\$'. User '\$username\$' has enabled file analysis for network connector '\$product\$'. User '\$username\$' has disabled file analysis for network connector '\$product\$'. User '\$username\$' has set param '\$param2\$' to '\$param3\$' for network connector '\$product\$'. User '\$username\$' has enabled file analysis mode '\$param1\$' for network connector '\$product\$'. |
| | Server Management | Network Connector added | 185 | Notice | User '\$user\$' has registered new network connector '\$param1\$', version '\$param2\$' |
| | Server Management | Network Connector removed | 186 | Notice | User '\$user\$' has removed network connector '\$param1\$', version '\$param2\$' |
| | Server Management | Notifier install failed | 156 | Error | Upgrade Error: Notifier for Policy '\$policyName\$', Setting '\$policySetting\$' was reset to default during upgrade. |
| | Server Management | Old events were deleted | 107 | Notice | Deleting \$param1\$ events older than \$param2\$. |
| ✦ | Server Management | Rapid Config created | 188 | Info | Rapid Config '\$param1\$' was created by '\$username\$'. |
| ✦ | Server Management | Rapid Config deleted | 189 | Info | Rapid Config '\$param1\$' was deleted by '\$username\$'. |
| ✦ | Server Management | Rapid Config disabled | 193 | Info | Rapid Config '\$param1\$' was disabled by '\$username\$'. |
| ✦ | Server Management | Rapid Config enabled | 192 | Info | Rapid Config '\$param1\$' was enabled by '\$username\$'. |
| ✦ | Server Management | Rapid Config modified | 190 | Info | Rapid Config '\$param1\$' was modified by '\$username\$'. |
| ✦ | Server Management | Rapid Config updated | 191 | Info | Rapid Config '\$param1\$' was updated by '\$username\$'. |
| | Server Management | Reporter restart | 151 | Warning | Reporter started, build information: \$param1\$. |
| | Server Management | Reporter shutdown | 152 | Notice | Reporter shutdown cleanly. |
| | Server Management | Server backup failed | 104 | Warning | Database backup has failed. |
| | Server Management | Server backup missed | 105 | Warning | Scheduled database backup was not performed. |
| | Server Management | Server backup started | 103 | Info | Database backup has been enabled, starting backup service. |
| | Server Management | Server backup stopped | 110 | Notice | Backup has been disabled, stopping backup service. |
| Δ | Server Management | Server Config List error | 113 | Error | Data is bad for config list entry. Id[\$param1\$], Version[\$param2\$], Data[\$param3\$]. Change Note: Capitalization of the subtype was changed in v8.1.0. |

| | Type | Subtype | ID No. | Severity | Example Descriptions/Comments |
|--------|-------------------|-----------------------------------|--------|-------------------|--|
| | Server Management | Server config modified | 102 | Notice | Configuration property '\$param1\$' was changed from '\$param3\$' to '\$param2\$' by '\$username\$'. Tracking of locally approved support files signed by Microsoft was disabled/enabled by '\$username\$' |
| ○ | Server Management | Server error | 142 | Error/ Warning | <i>There are too many descriptions to list for this subtype since it handles many different types of errors. Examples include:</i> Carbon Black File Reputation - error logged and service resuming operation. The remote server returned an unexpected response: (413) Request Entity Too Large. Change Note: CB Collective Cloud Defense replaced with Carbon Black File Reputation in v8.5.0. |
| | Server Management | Server performance | 175 | Warning | Event filter for alert '\$alertName\$' is not performing well. Execution took \$param2\$ ms while processing \$param3\$ events. Please review associated alert filter. Event Rule '\$ruleName1\$' is not performing well. Execution took \$param2\$ ms while processing \$param3\$ events. Please review associated Event Rule filter. |
| Ⓜ | Server Management | Server restart | 101 | Notice | Carbon Black App Control Server started, build information: \$param1\$. Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0. |
| Ⓜ | Server Management | Server shutdown | 100 | Warning | Carbon Black App Control Server shutdown cleanly. Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0. |
| ⚡ Ⓜ | Server Management | Server upgrade failed | 112 | Error | Failed to upgrade Carbon Black App Control Server to \$param1\$. Contact support. Change Note: The event description referred to "Parity Server" or "Bit9 Server" in pre-8.0.0 releases. Not currently used in v8.0.0. Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0. |
| ★ Ⓜ | Server Management | Server upgrade info | 195 | Info | Upgrade Information for server Carbon Black App Control Server : Default Rules order was modified by customer. Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0. |
| ⚡ Ⓜ | Server Management | Server upgrade succeeded | 111 | Info | Successfully upgraded Carbon Black App Control Server to version \$param1\$. Change Note: The event description referred to "Parity Server" or "Bit9 Server" in pre-8.0.0 releases. Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0. |
| | Server Management | SSL certificate CN mismatch | 128 | Critical | Common Name mismatch between SSL certificate (\$param1\$) and RPC Server Name (\$param2\$). |
| | Server Management | SSL certificate error | 127 | Critical | Server was not able to use default SSL certificate. Communication with agents is disabled. |
| | Server Management | SSL certificate expired | 125 | Critical | Server SSL certificate has expired on \$param1\$. Agents will not be able to connect if SSL protocol is enabled. |
| | Server Management | SSL certificate expiring | 124 | Critical | Server SSL certificate will expire on \$param1\$. |
| Ⓜ | Server Management | SSL certificate generated | 118 | Notice | User '\$username\$' has successfully generated a new SSL certificate for Carbon Black App Control Server: \$param1\$ Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0. |
| Ⓜ | Server Management | SSL certificate generation failed | 119 | Warning | User '\$username\$' has failed to generate a new SSL certificate for Carbon Black App Control Server. Error: \$param1\$ Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0. |
| Ⓜ | Server Management | SSL certificate import failed | 121 | Warning | User '\$username\$' has failed to import new SSL certificate for Carbon Black App Control Server. Error: \$param1\$ Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0. |
| Ⓜ | Server Management | SSL certificate imported | 120 | Notice | User '\$username\$' has successfully imported a new SSL certificate for Carbon Black App Control Server: \$param1\$ |

| | Type | Subtype | ID No. | Severity | Example Descriptions/Comments |
|--------|--------------------------|------------------------------------|--------|----------|---|
| | | | | | Change Note: CB Protection replaced with Carbon Black App Control in v8.5.0. |
| | Server Management | Strong SSL communications disabled | 123 | Warning | User '\$username\$' has disabled strong SSL communications. Agents using strong SSL will not be able to talk to server anymore. Contact Carbon Black Support for remediation. |
| | Server Management | Strong SSL communications enabled | 122 | Notice | User '\$username\$' has enabled strong SSL communications. Server cannot be spoofed. |
| | Server Management | System error | 137 | Error | Reports a variety of descriptions for command line usage errors in rarely used debugging activities. |
| + | Server Management | Unified server added | 280 | Info | Unified server '\$param1\$' added to local configuration by '\$username\$'. |
| + | Server Management | Unified server error | 283 | Critical | Unified server '\$param1\$' inaccessible. Unified server '\$param1\$' inaccessible due to an issue with the SSL certificate. Unified server '\$param1\$' inaccessible due to an authentication issue. |
| + | Server Management | Unified server modified | 282 | Info | Unified server '\$param1\$' modified by '\$username\$'. Unified Management disabled on local server by '\$username\$'. Unified Management configured to be managed only from this server by '\$username\$'. Unified Management configured to be managed from all servers by '\$username\$'. This server was added to remote unified management configuration by '\$username\$'. |
| + | Server Management | Unified server removed | 281 | Info | Unified server '\$param1\$' removed from local configuration by '\$username\$'. |
| | Server Management | Updater created | 145 | Info | Updater '\$updaterName\$' was created by '\$username\$' |
| | Server Management | Updater deleted | 146 | Info | Updater '\$updaterName\$' was deleted by '\$username\$' Note: There is a separate Enabled Updater deleted event for Updaters deleted while enabled. |
| | Server Management | Updater modified | 147 | Info | Updater '\$updaterName\$' was modified by '\$username\$'. Enabled Updater '\$updaterName\$' was deleted by '\$username\$'. |
| | Server Management | Updaters Indicator Set disabled | 171 | Info | '\$username\$' disabled automatic update of Indicator Sets from Carbon Black File Reputation |
| | Server Management | Updaters Indicator Set enabled | 170 | Info | '\$username\$' enabled automatic update of Indicator Sets from Carbon Black File Reputation |
| Δ | Server Management | Updaters update disabled | 150 | Info | '\$username\$' disabled automatic update of Application Updaters from Carbon Black File Reputation Change Note: Capitalization of the subtype was changed in v8.1.0. |
| Δ | Server Management | Updaters update enabled | 149 | Info | '\$username\$' enabled automatic update of Application Updaters from Carbon Black File Reputation Change Note: Capitalization of the subtype was changed in v8.1.0. |
| + | Server Management | Yara Rules Added | 197 | Info | A new set of Yara Rules were added: \$param1\$ Version: \$param2\$. |
| + | Server Management | Yara Rules Modified | 198 | Info | Yara Rules were modified: \$param1\$ OldVersion: \$param2\$. |
| | Session Management | Console user created | 302 | Info | '\$userName1\$' created new username '\$userName2\$'. |
| | Session Management | Console user deleted | 303 | Info | '\$userName1\$' deleted the user '\$userName2\$'. |
| Δ ◇ | Session Management | Console user login | 300 | Info | User '\$username\$' logged in from \$ipaddress\$. User '\$username\$' logged in from \$ipaddress\$ via SAML. User '\$username\$' redirected to unified server \$serverName\$. Change Note: In v8.0.0, a new description option for Unified Management was added. In v8.1.0, a new description option was added for SAML logins. |
| | Session Management | Console user logout | 301 | Info | User '\$username\$' logged out. |
| ◇ | Session Management | Console user modified | 304 | Info | '\$userName1\$' changed the User Roles for '\$userName2\$'. '\$userName1\$' changed the password for '\$userName2\$'. |

| | Type | Subtype | ID No. | Severity | Example Descriptions/Comments |
|---|--------------------|----------------------------|--------|----------|---|
| | | | | | <p>'\$UserName1\$' modified the user '\$UserName2\$'.</p> <p>'\$UserName1\$' changed the password for '\$UserName2\$'.</p> <p>'\$UserName1\$' created the API token for '\$UserName2\$'.</p> <p>Unified server modified the unified user \$UserName2\$.</p> <p>Change Note: In pre-8.0.0 releases, the first description referred to "access level" instead of user roles, and listed the user group the user was moved from and to. User groups were changed to user roles in v8.0.0, and users can have more than one role. Also, unified servers are new for v8.0.0; the "Unified server modified" message indicates that a user has been authenticated on a client server.</p> |
| | Session Management | Multiple failed logins | 305 | Warning | User '\$username\$' has failed to login \$param1\$ times in a row. Current IP Address \$ipaddress\$. |
| ✦ | Session Management | User Role AD rules changed | 309 | Notice | '\$username\$' modified an AD rule for mapping \$param1\$ to the User Role \$param2\$. |
| ◇ | Session Management | User Role created | 306 | Info | User Role '\$param1\$' created by '\$username\$'. |
| ◇ | Session Management | User Role deleted | 307 | Info | User Role '\$param1\$' deleted by '\$username\$'. |
| ◇ | Session Management | User Role modified | 308 | Info | User Role '\$param1\$' modified by '\$username\$'. |
| | | | | | Change Note: Prior to v8.0.0, the event subtype and description referred to "User group". |

Section 2: Access to Event Data

In addition to the App Control Console user interface, event data is available in the following ways:

- as Syslog output, in one of four formats
- as App Control “external event logging” output
- as SQL views through the App Control “Live Inventory SDK”
- as JSON output to external analytics services
- in event archive files

Syslog Formats

App Control supports integration of its event information with Syslog servers using several formats. You configure Syslog integration on the Events tab of the System Configuration page, described in the “System Configuration” chapter of the *App Control User Guide* or in online Help in the App Control Console. Upgrades from previous releases retain the format setting they had.

The supported formats are:

- **Basic (RFC3164)** – the default for upgrades from some previous releases
- **Enhanced (RFC5424)** – a newer standard; the default for new installations
- **CEF (HP ArcSight)** – the format to use to integrate App Control event logs with [HP ArcSight ESM](#) or [HP ArcSight Logger](#)
- **LEEF (IBM Q1 Labs)** – the format to use to integrate App Control event logs with [IBM Security QRadar Log Manager](#) or [IBM Security QRadar SIEM](#)

Note: Manually enabled, custom Syslog formatting will be overwritten on upgrade to this version of App Control. See “Setting Up External Event Logging” in the *App Control User Guide* for instructions on configuring the App Control Server for CEF syslog formatting.

Basic and Enhanced Standard Syslog Formats

The fields available in Basic and Enhanced Standard Syslog formats are the same, except for three optional fields – App-Name, ProclD, and MsgID. [Table 4](#) shows the Basic and Enhanced Syslog format fields supported by App Control. Examples of messages in these formats are shown below the table.

Table 4. App Control Event Mapping to Basic and Enhanced Syslog Formats

| Syslog field | Data Type | Note |
|-----------------------|---------------|---|
| Facility ¹ | INTEGER | Syslog facility, always “user-level” Note: Facility and Severity are coded into one number per Syslog specification. |
| Severity ¹ | INTEGER | Severity mapped from event severity (see Error! Reference source not found.) Note: Facility and Severity are coded into one number per Syslog specification. |
| Version | INTEGER | (Enhanced Syslog only) Syslog version, by default “1” |
| Timestamp | DATETIME | Timestamp when the Syslog event was sent (with the year and UTC time zone according to RFC 5424) |
| Hostname | NVARCHAR(256) | App Control Server hostname, appended by domain as per RFC 5424 |

| Syslog field | | Data Type | Note |
|--------------|--|---|---|
| App-Name | | NVARCHAR(256) | (Enhanced Syslog only) Configurable value in ParityReporter.log.xml, by default “-“ |
| ProclD | | NVARCHAR(256) | (Enhanced Syslog only) Configurable value in ParityReporter.log.xml, by default “-“ |
| MsgID | | NVARCHAR(256) | (Enhanced Syslog only) Configurable value in ParityReporter.log.xml, by default “-“. |
| Message | Message field | | Message is a long text string beginning with <i>event:</i> and including all the “All messages” fields below inline; the message also can include some combination of the conditional fields. Carbon Black App Control Server event:text=“...” type=“...” ... |
| | Text | NVARCHAR(2048) | Event message (All messages) |
| | Type | NVARCHAR(256) | Event type name (All messages) |
| | subtype | NVARCHAR(256) | Event subtype name (All messages) |
| | hostname | NVARCHAR(256) | Event source – computer name or 'System' for App Control Server (All messages) |
| | username | NVARCHAR(256) | Name of user associated with the event (All messages) |
| | date | DATETIME | Event timestamp in UTC (All messages) |
| | ip_address | VARCHAR | IP address (IPv4 or IPv6) of the agent reporting the event (Conditional) |
| | process | NVARCHAR(512) | Process associated with the event (Conditional) |
| | file_path | NVARCHAR(450) | File path of the file associated with the event (Conditional) |
| | file_name | NVARCHAR(450) | Name of the file associated with the event (Conditional) |
| | file_hash | CHAR(64) | Hash of the file associated with the event (Conditional) |
| | installer_name | NVARCHAR(450) | Name of the Installer associated with the event (e.g., the installer that installed a newly discovered file) (Conditional) |
| | policy | NVARCHAR(128) | Name of the App Control policy for the agent associated with the event (Conditional) |
| | ban_name | NVARCHAR(128) | For files blocked due to bans, name of the ban (Conditional) |
| | Rapid_config_name | NVARCHAR(256) | Name of the Rapid Config associated with the event (Conditional) |
| | rule_name | NVARCHAR(256) | Name of the rule associated with the event (Conditional) |
| | updater_name | NVARCHAR(256) | Name of the Updater associated with the event (Conditional) |
| | indicator_name | NVARCHAR(256) | Name of the threat indicator associated with the event; if present, same as rule_name (Conditional) |
| | server_version | NVARCHAR(MAX) | Version of the App Control Server associated with the event (All messages) |
| file_trust | -2 pending -1 unknown 0-10 Trust value | File trust from the Carbon Black File Reputation of the file associated with the event. Pending implies that FILE lookup was not yet performed but will be. (Conditional) | |
| file_threat | -2 pending -1 unknown | File threat from Carbon Black File Reputation of the file associated with the event. Pending implies that Carbon | |

| Syslog field | Data Type | Note |
|-----------------------------------|--|---|
| | 0 No threat 1 Potential risk 2 Malicious | Black File Reputation lookup was not yet performed but will be. (Conditional) |
| Message fields (continued) | | |
| process_key | UID | |
| process_trust | -2 pending -1 unknown 0-10 Trust value | Unique proprietary key identifying the instance of the process on a specific computer |
| process_threat | -2 pending -1 unknown 0 No threat 1 Potential risk 2 Malicious | Parent process trust from Carbon Black File Reputation of the file associated with the event. Pending implies that Carbon Black File Reputation lookup was not yet performed but will be. (Conditional) |
| unified_source | NVARCHAR(256) | Unified server that is the source of and event, if unified management is enabled and the source of an event. (Conditional; new in v8.0.0) |

Basic Syslog Format Message

The following is an example of Basic Syslog format:

```
16/06/16 13:42:48
Info message from: 123.45.67.8
Hostname: desktop8.mycorp.local
Carbon Black App Control event: text="File 'c:\apps\alexainstaller.exe'
[07693beb9aaebdd8b3223a5becc25b44c70afd73cec9e4984ffc4e89624c5e17] was
executed for the first time." type="Discovery" subtype="First execution on
network" hostname="WORKGROUP\LAPTOP6" username="LAPTOP6\Administrator"
date="6/16/2016 1:42:48 PM" ip_address="fd70::a98b:d49b:e45f:cd30"
process="c:\windows\explorer.exe" file_path="c:\apps\alexainstaller.exe"
file_name="alexainstaller.exe"
file_hash="07693beb9aaebdd8b3223a5becc25b44c70afd73cec9e4984ffc4e89624c5e17"
policy="Test" process_key="00000000-0000-0574-01cf-86e9e504f7e6"
server_version="8.1.0.899" file_trust="0" file_threat="2" process_trust="10"
process_threat="0"
```

Enhanced Syslog Format Message

The following is an example of Enhanced Syslog format:

```
16/06/16 14:38:37
Notice message from 123.45.67.8
Hostname: desktop8.mycorp.local
1 2016-06-16T14:38:37Z laptop6 - - - Carbon Black App Control event:
text="Computer WORKGROUP\LAPTOP6 discovered new file
'c:\windows\temp\jvyyqbe4.dll'
[eeb0ada676b1f8e5e94015b5e48ed4bcf23959b0d0837bbd51c1870f5d641d2a]."
type="Discovery" subtype="New unapproved file to computer"
hostname="WORKGROUP\LAPTOP6" username="NT AUTHORITY\SYSTEM" date="6/16/2016
2:38:35 PM" ip_address="fd70::a98b:d49b:e45f:cd30"
process="c:\windows\microsoft.net\framework64\v2.0.50727\csc.exe"
file_path="c:\windows\temp\jvyyqbe4.dll" file_name="jvyyqbe4.dll"
file_hash="eeb0ada676b1f8e5e94015b5e48ed4bcf23959b0d0837bbd51c1870f5d641d2a"
installer_name="csc.exe" policy="Test" process_key="00000000-0000-0bc4-01cf-
8970a7aca018" server_version="8.1.0.992" file_trust="-1" file_threat="-1"
```

Mapping App Control Events to ArcSight CEF

App Control supports integration of its event information with Syslog servers using several formats. One of the Syslog formats supported is ArcSight CEF (Common Event Format), which you can use to integrate App Control event logs with ArcSight ESM or ArcSight Logger. You configure Syslog integration on the System Configuration/Events page, described in the “System Configuration” chapter of *Using App Control*.

This section describes the mapping of App Control event fields to ArcSight CEF fields. See your ArcSight documentation for full information about ArcSight CEF and its capabilities.

Top-Level Syslog Format

Table 5. App Control Event Mapping to Syslog ArcSight Common Event Format (RFC 3164 and ArcSight CEF)

| Syslog field | Data Type | Note |
|--------------|---------------|--|
| Facility | INTEGER | Syslog facility; always “user-level” Note: Facility and Severity are coded into one number per Syslog specification. |
| Severity | INTEGER | Severity mapped from event severity (see Table 2) Note: Facility and Severity are coded into one number per Syslog specification. |
| Timestamp | DATETIME | Timestamp when the Syslog event was sent (without the year, according to RFC 3164) |
| Hostname | NVARCHAR(256) | App Control Server hostname |
| Message | | Message encoded according to ArcSight CEF specification |

Message Format

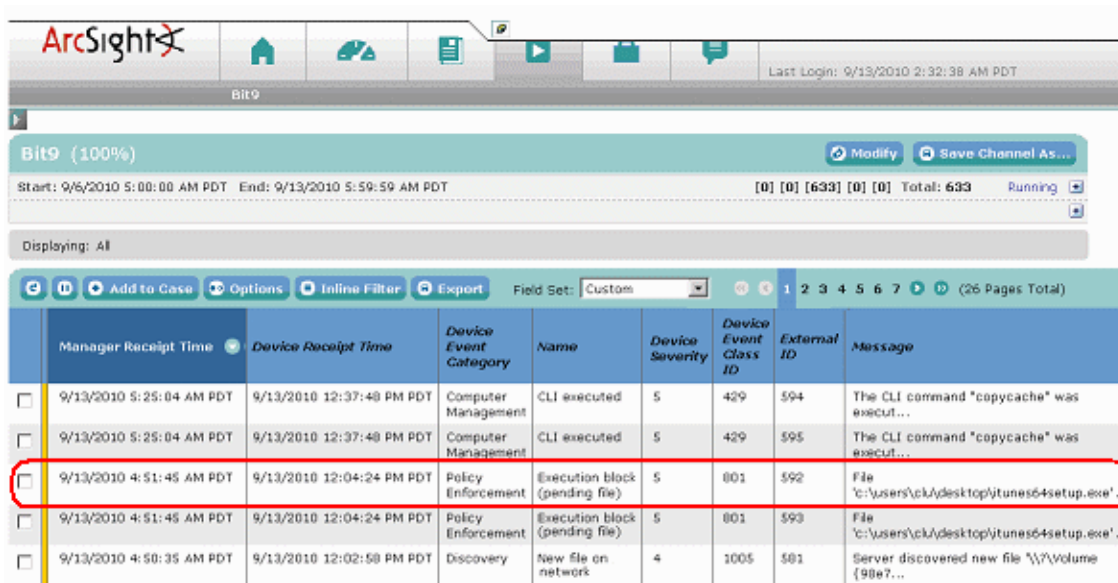
ArcSight CEF format uses the Syslog message protocol as a transport mechanism. The format of the message is:

```
Date-Time host CEF:Version|Device Vendor|Device Product|Device Version|
SignatureID|Name|Severity|Extension
```

Each message includes a common prefix consisting of the message date and time, the hostname of the server from which it was sent, and "CEF:" plus the version of CEF format. The remainder of the message is formatted into event-specific fields delimited by a bar ("|") character.

The following example illustrates a CEF-formatted message using Syslog output from App Control:

```
Sep 19 08:26:10 server3.mycorp.local CEF:0|Carbon Black|Protection
|8.1.0.899|801|Execution block (unapproved file)|5| dst=10.0.0.1
duser=NTAUTHORITY\SYSTEM msg=File 'itunessetup64.exe' has been blocked
because it was unapproved.
```



CEF-App Control Mapping Tables

The tables below provide the following CEF-App Control mapping information:

- [Table 6](#) shows the mapping of App Control data to CEF Header fields
- [Table 7](#) shows the mapping of App Control data to CEF Extension field data
- [Table 8](#) shows App Control-specific custom extensions

Table 6. Mapping of App Control Event Data to CEF Header Fields

| CEF Prefix Field | App Control Value | Description |
|------------------|--------------------|--|
| Host | Hostname | Hostname of the App Control Server providing the Syslog output. |
| Version | 0 | CEF format version. By default this is 0. |
| Device Vendor | Carbon Black | The company name of the syslog output provider. |
| Device Version | 8.5.0.xxx | The version of product generating syslog output. The current App Control version is 8.5.0 and xxx represents the build number appended to the version. |
| Device Product | Protection | The product name of the syslog output provider. |
| SignatureID | Event subtype ID | Unique number for the event subtype as classified by App Control. |
| Name | Event subtype name | Unique name for the event subtype as classified by App Control. |

| | | |
|-----------|-------------------|---|
| Severity | Event severity ID | Numeric value indicating the severity of the event. App Control event severity ranges from 7 (least severe) to 0 (most severe). These are mapped to CEF severity levels, which range from 0 (least severe) to 10 (most severe). The CEF severity is calculated by subtracting the App Control severity from 9. This means that the most severe App Control event has a CEF severity of 9. The least severe App Control event has a CEF severity of 2. |
| Extension | <i>(varies)</i> | Additional event information. See Table 7 . |

Table 7. Mapping of App Control Event Data to CEF Extensions

| CEF Extension Name | App Control Event Field | Description |
|----------------------------|--------------------------|---|
| externalId | Event ID | Unique auto-incremented ID of each generated App Control event. |
| DeviceEventCategory | Event Type | App Control event type |
| startTime | Event Timestamp | Timestamp when the event was created on the endpoint (in UTC). |
| ReceiptTime | Event Received Timestamp | Timestamp when the event was received by the App Control Server (in UTC). |
| Message | Event Description | Full text message of the App Control event |
| deviceHostName | Server Hostname | App Control Server host name. Note that this could be an IP address if that is what was entered during server installation. |
| destinationAddress * | IP Address | IPv4 address of the machine generating the event (if available). |
| deviceCustomIPv6Address3 * | IP Address | Ipv6 address of the machine generating the event (if available). |
| destinationHostName * | Hostname | Host name of the machine generating the event. |
| destinationUserName * | Username | User name of the user generating the event. |
| FileId * | Antibody ID | Unique (auto-incremented) ID of the file generating the event. |
| filePath * | File Path | Full pathname of the file generating the event. |
| fileName * | File Name | Filename of the file generating the event. |
| fileHash * | File Hash | SHA-256 file hash of the file generating the event. |
| deviceProcessName * | Process | Process name of the process generating the event. |

| CEF Extension Name | App Control Event Field | Description |
|--|-------------------------|---|
| sourceProcessName | Process Key | Unique proprietary key identifying the instance of the process on a specific computer |
| reason | Indicator Name | Name of the threat indicator associated with the event; if present, same as rule name (Conditional) |
| deviceExternalID | Unified Source | Name of the unified management server that is the source of an event (Conditional) |
| * CEF Extensions with asterisks are context-dependent and not available on all events. | | |

Table 8. Mapping to Custom CEF Extensions

| CEF Custom Extension & Label | App Control Event Field | Description |
|---|-------------------------|--|
| deviceCustomString1 * deviceCustomString1Label = "rootHash" | Root Hash | Root hash of the file generating the event. |
| deviceCustomString2 * deviceCustomString2Label = "installerFilename" | Installer Filename | Installer Filename of the file generating the event. |
| deviceCustomString3 * deviceCustomString3Label = "policy" | Policy | App Control policy of the machine generating the event. |
| deviceCustomString 4* deviceCustomString4Label = "banName" | Ban Name | For a block event, the name of the ban (if any) that blocked the file; some bans are unnamed |
| deviceCustomString 5* deviceCustomString5Label = "ruleName" | Rule Name | The name of the rule associated with the event (if any) |
| deviceCustomString 6* deviceCustomString6Label = "updaterName" | Updater Name | The name of the Updater associated with the event (if any) |

| CEF Custom Extension & Label | App Control Event Field | Description |
|--|-------------------------|--|
| deviceCustomFloatingPoint1 * deviceCustomFloatingPoint1Label = "fileTrust" | File Trust | File trust from Carbon Black File Reputation of the file associated with the event. Pending means that Carbon Black File Reputation lookup was not yet performed but will be. (Conditional) -2 pending -1 unknown 0-10 Trust value |
| deviceCustomFlexString1 * deviceCustomFlexString1Label = "fileThreat" | File Threat | File threat from Carbon Black File Reputation of the file associated with the event. Pending means that Carbon Black File Reputation lookup was not yet performed but will be. (Conditional) "pending" "unknown" "0 - No threat" "1 - Potential risk" "2 - Malicious" |
| deviceCustomFloatingPoint2 * deviceCustomFloatingPoint2Label = "processTrust" | Process Trust | Parent process trust from Carbon Black File Reputation of the file associated with the event. Pending means that Carbon Black File Reputation lookup was not yet performed but will be. (Conditional) -2 pending -1 unknown 0-10 Trust value |
| deviceCustomFlexString2* deviceCustomFlexString2Label = "processThreat" | Process Threat | Parent process threat from Carbon Black File Reputation of the file associated with the event. Pending implies that Carbon Black File Reputation lookup was not yet performed but will be. (Conditional) "pending" "unknown" "0 - No threat" "1 - Potential risk" "2 - Malicious" |
| * All CEF Custom Extensions are context-dependent and not available on all events. | | |

Mapping App Control Events to Q1Labs LEEF Format

One of the Syslog formats supported by App Control is Q1Labs LEEF (Log Event Extended Format), which you can use to integrate App Control event logs with QRadar SIEM or QRadar Log Manager. You configure Syslog integration on the System Configuration page Events tab in the App Control Console.

This section describes setup of QRadar Log Manager to accept App Control events, and the mapping of App Control event fields to Q1Labs LEEF fields. See your QRadar documentation for full information about QRadar and LEEF capabilities.

Important: If you are running **App Control version 8.1.0 or later**, you must update the **QRadar DSM** module for App Control to at least the **July 2017** version released by QRadar. This will enable QRadar to

properly parse App Control 8.0- and 8.1-specific events. The previous DSM module for Bit9 Security Platform can still be used to integrate older versions of the Bit9 product with the QRadar.

Configuring QRadar Log Manager

When an App Control Server begins to send events to the QRadar Log Manager, approximately the first 10 events will appear as "Unknown events". After that, QRadar Log Manager will auto-discover events as being from Carbon Black App Control, and will add a Log source definition for that App Control Server called "CarbonBlackAppControl @ <CarbonBlackServerComputerName>" with the default QRadar Log Manager parameters.

To be certain you capture all events, set up Carbon Black App Control as a log source in QRadar Log Manager *before* integrating with the Carbon Black App Control Server.

Manual Setup of App Control as Event Source

You can manually configure App Control as the source of events sent to the QRadar Log Manager.

To configure Carbon Black App Control as an event source for QRadar Log Manager:

1. In the QRadar Log Manager Console, click on the **Admin** tab.
2. On the console Admin settings, under Data Sources/Events, click **Log Sources**. The Log Sources window opens.
3. In the Log Source window menu bar, click **Add**. The Add a Log Source window opens.
4. In the new window, for Log Source Name, enter **Carbon Black App Control**.
5. For Log Source Description, enter **Carbon Black App Control Server**.
6. Choose **Carbon Black App Control** on the Log Source menu.
7. For Log Source Identifier, enter the fully qualified domain name of the Carbon Black App Control Server sending the events.
8. Set Credibility to **10**.
9. Click the **Save** button.
10. On the QRadar Log Manager Admin console, click **Deploy Changes** in the Admin menu bar.

Top-Level Syslog Format

Table 9. App Control Event Mapping to Q1Labs Log Event Enhanced Format (RFC 3164 and Q1Labs LEEF)

| Syslog field | Data Type | Note |
|------------------|---------------|---|
| Facility | INTEGER | Syslog facility; always "user-level" Note: Facility and Severity are coded into one number per Syslog specification. |
| Severity | INTEGER | Severity mapped from App Control event severity (see Table 2) Note: Facility and Severity are coded into one number per Syslog specification |
| Timestamp | DATETIME | Timestamp when the Syslog event was sent (without the year, according to RFC 3164) |
| Hostname | NVARCHAR(256) | App Control Server hostname |
| Message | | Message encoded according to Q1Labs LEEF specification |

LEEF Format

Q1Labs LEEF format uses the Syslog message protocol as a transport mechanism. The format of the message is:

```
Date-Time hostname LEEF:Version|Vendor|Product|Version|EventID|
Key1=Value1<tab>Key2=Value2<tab>...<tab>KeyN=ValueN
```

Each message includes a common prefix consisting of the message date and time, the hostname of the server from which it was sent, and "LEEF:" plus the version of LEEF format. Following the prefix, the message includes fields describing the product sending the message and an event identifier. The remainder of the message is formatted into an event-specific series of key value pairs delimited by a tab character. Characters in the message are UTF-8 encoded.

The following example illustrates a LEEF-formatted message using Syslog output from App Control, with "<tab>" substituted where actual tabs are used in the message:

```
Jan 18 11:07:53 198.76.5.4 LEEF:1.0|Carbon_Black|Protection|
8.1.0.978<tab>|NEW_PORT_DISCOVERD|src=172.5.6.67<tab>dst=172.50.123.1<tab>
sev=5<tab>cat=anomaly<tab>msg=there are spaces in this message
```

App Control-to-LEEF Mapping Tables

The tables below provide the following LEEF-App Control mapping information:

- [Table 10](#) shows the mapping of App Control event data to LEEF Header fields
- [Table 11](#) shows the mapping of App Control events to LEEF Attributes

Table 10. Mapping of App Control Event Data to LEEF Header Fields

| LEEF Prefix Field | App Control Value | Description |
|-------------------|--------------------|--|
| Hostname | Hostname | Hostname of the App Control Server providing the Syslog output |
| LEEF Version | 1.0 | LEEF format version. By default this is 1.0. |
| Vendor | Carbon Black | The company name of the Syslog output provider. |
| Product* | Protection | The name of the product generating Syslog output. |
| Version | 8.5.0.xxx | The version of the product generating Syslog output, including the build number (represented here by "xxx"). The current App Control version is 8.5.0. |
| EventID | Event subtype name | Unique name identifying the event subtype as classified by Carbon Black App Control. |
| Attributes | (varies) | See Table 11 . |

Table 11. Mapping of App Control Event Fields to LEEF Attributes

| LEEF Attribute (name in RAW view) | LEEF Property (Visible name in Console) | Regular Expression (to Extract) | App Control Event Field | Description |
|-----------------------------------|---|---------------------------------|-------------------------|---|
| cat | Category | | Event Type | App Control event category name |
| sev | Severity | | Severity | Severity of the App Control event. Mapped from App Control range 7-0 (0 is most important) into LEEF range 1-10 (10 = most important) |
| devTime | Device Time | | Event Timestamp | Timestamp (UTC) when App Control event was generated; Converted to local time when displayed as "Log Source Time" in QRadar events view |
| receivedTime ¹ | Received Time | receivedTime=([\t+)[\t]* | Received Time | Timestamp (UTC) when the event was received by the App Control Server |
| msg ¹ | Message | msg=([\t+)[\t]* | Event Description | Full message describing the event |
| externalID ¹ | External ID | externalId=([\t+)[\t]* | Event Id | Unique identifier of the event instance |
| src ² | Source Address | | Ip Address | IP (IPv4) address of the computer generating the event |
| srcHostName ^{1,2} | Source Hostname | srcHostName=([\t+)[\t]* | Hostname | Hostname of the computer generating the event |
| srcProcess ^{1,2} | Source Process | srcProcess=([\t+)[\t]* | Process | Name of the process generating the event |
| usrName ² | Username | | Username | Username of the user generating the event |
| filePath ^{1,2} | File Path | filePath=([\t+)[\t]* | File Path | Full path of the file generating the event |
| fileName ^{1,2} | Filename | fileName=([\t+)[\t]* | File Name | Filename of the file generating the event |
| fileHash ^{1,2} | File Hash | fileHash=([\t+)[\t]* | File Hash | SHA256 hash of file generating the event |
| fileId ^{1,2} | File ID | fileId=([\t+)[\t]* | Antibody Id | Unique identifier of file generating the event |
| rootHash ^{1,2} | Root Hash | rootHash=([\t+)[\t]* | Root Hash | Root hash of the file generating the event |

| LEEF Attribute (name in RAW view) | LEEF Property (Visible name in Console) | Regular Expression (to Extract) | App Control Event Field | Description |
|---|---|------------------------------------|----------------------------------|--|
| installerFileName ^{1,2} | Installer Filename | installerFileName=([^\t+)]\t]* | Installer Filename | Installer filename of the file generating the event |
| banName ^{1,2} | Ban Name | banName=([^\t+)]\t]* | Ban Name | For block events, name of the ban that blocked the file. Change Notes: This was "ruleName" prior to 7.0.1 Patch 3. |
| ruleName ^{1,2} | Rule Name | ruleName=([^\t+)]\t]* | Rule Name | Name of the rule associated with the event (if any) |
| updaterName ^{1,2} | Updater Name | updaterName=([^\t+)]\t]* | Updater Name | Name of the Updater associated with the event (if any) |
| indicatorName | indicatorName | indicatorName=([^\t+)]\t]* | Indicator Name | Name of the threat indicator associated with the event (if any) |
| policy ^{1,2} | Policy | policy=([^\t+)]\t]* | Policy | App Control Policy of the computer generating the event |
| dstHostName ¹ | Destination Hostname | dstHostName=([^\t+)]\t]* | Hostname | App Control Server computer receiving the event |
| processKey | Process Key | processKey=([^\t+)]\t]* | Process Key | Unique proprietary key identifying the instance of the process on a specific computer |
| fileTrust | File Trust | fileTrust=([^\t+)]\t]* | File Trust | File trust from Carbon Black File Reputation of the file associated with the event. Pending implies that file lookup was not yet performed but will be. (Conditional) -2 pending -1 unknown 0-10 Trust value |

| LEEF Attribute (name in RAW view) | LEEF Property (Visible name in Console) | Regular Expression (to Extract) | App Control Event Field | Description |
|--|---|------------------------------------|----------------------------------|--|
| fileThreat | File Threat | fileThreat=([^\t+][\t]* | File Threat | File threat from Carbon Black File Reputation of the file associated with the event. Pending implies that file lookup was not yet performed but will be. (Conditional) -2 pending -1 unknown 0 No threat 1 Potential risk 2 Malicious |
| processTrust | Process Trust | processTrust=([^\t+][\t]* | Process Trust | Parent process trust from Carbon Black File Reputation of file associated with the event. Pending implies that file lookup was not yet performed but will be. (Conditional) -2 pending -1 unknown 0-10 Trust value |
| processThreat | Process Threat | processThreat=([^\t+][\t]* | Process Threat | Parent process threat from Carbon Black File Reputation of file associated with the event. Pending implies that file lookup was not yet performed but will be. (Conditional) -2 pending -1 unknown 0 No threat 1 Potential risk 2 Malicious |
| unifiedSource | Unified Source | unifiedSource=([^\t+][\t]* | Unified Server Source | Hostname of the Unified Server (if implemented) that is the source of an event |
| <p>¹These are custom LEEF attributes for App Control event fields with no predefined attribute name in LEEF. You must use the regular expressions next to each of these items to extract it as a custom attribute. See Manual Setup of App Control Custom Properties for instructions.</p> <p>² These LEEF Extensions are context-dependent and not available on all events.</p> | | | | |

Manual Setup of App Control Custom Properties

For the current release of QRadar Log Manager, manual setup is required to parse certain App Control properties. [Table 11](#) shows the regular expressions that must be used to parse each custom property.

To configure custom properties for QRadar Log Manager:

1. On the QRadar Log Manager, click the **Admin** tab and then click **Custom Event Properties** in the Data Sources/Events section. The Custom Event Properties window opens.
2. Click **Add** in the Custom Event Properties window menu bar. The Event Property Definition window opens.
3. In the Event Property Definition window, click the **New Property** radio button, and in the New Property text box, enter a LEEF Property name from [Table 11](#) (such as “Message”).
4. Choose **App Control** on the Log Source Type menu.
5. Enter the regular expression from [Table 11](#) corresponding to the property you chose (such as “`msg=([^\t]+)[\t]*`”).
6. Make sure that the **Enabled** box is checked, and then click the **Save** button.
7. Repeat the steps above for each App Control custom property (those with regular expressions) listed in [Table 11](#).
8. On the Admin console, click **Deploy Changes** in the Admin menu bar.

External Event Database

You can send events from the App Control Server to an external database. The following table describes the external events table columns.

Table 12. App Control External Event Database Columns

| External table column | Data Type | Note |
|-----------------------|----------------|---|
| event_id | BIGINT | ID of the event |
| time | DATETIME | Time when event occurred (in UTC) |
| received_time | DATETIME | Time when server received the event (in UTC) |
| severity | NVARCHAR(256) | Event severity |
| priority | NVARCHAR(256) | Event severity; note that priority was used in pre-7.2.1 releases, and is deprecated for 7.2.1 and later. The preferred name is "severity". |
| type | NVARCHAR(256) | Event type name |
| subtype | NVARCHAR(256) | Event subtype name |
| text | NVARCHAR(1024) | Event description |
| hostname | NVARCHAR(128) | Event source (computer name or 'system') |
| host_id | INTEGER | ID of the event source (computer ID or 0 for 'system') |
| ip_address | VARCHAR(40) | IP address associated with the event |
| platform | NVARCHAR(64) | Platform of the computer associated with the event (Windows, Mac, Linux) |
| hostgroup | NVARCHAR(512) | Name of the policy associated with the event |
| hostgroup_id | INTEGER | ID of the policy associated with the event |
| username | NVARCHAR(512) | Name of user associated with the event |
| process | NVARCHAR(512) | Name of the process associated with the event |
| filename | NVARCHAR(1024) | Full file path |
| hash | CHAR(64) | File hash (sha256) |
| tail_filename | NVARCHAR(256) | Truncated file name (max. 256 characters) |
| roothash | CHAR(64) | Installer hash (sha256) |
| rootname | NVARCHAR(1024) | Installer name associated with the event |
| ieid | INTEGER | Installer ID associated with the event |
| ban_name | NVARCHAR(128) | For blocked file events, the name of the ban that blocked the file action; some bans are unnamed |
| rule_name | NVARCHAR(128) | Name of the rule associated with the event (if any) |
| updater_name | NVARCHAR(256) | Name of the Updater associated with the event (if any) |
| parent_id | INTEGER | Not used |
| indicator_name | NVARCHAR(128) | Name of the threat indicator associated with the event (if any) |
| process_key | NVARCHAR(128) | Unique proprietary key identifying the instance of the process on a specific computer |
| file_trust | INTEGER | File trust from Carbon Black File Reputation of the file associated with the event. Pending means that file lookup was not yet performed but will be. (Conditional) -2 pending -1 unknown |

| | External table column | Data Type | Note |
|------------------------------|-----------------------|-----------------|---|
| | | | 0-10 Trust value |
| | file_threat | INTEGER | File threat from Carbon Black File Reputation of the file associated with the event. Pending means that file lookup was not yet performed but will be. (Conditional) -2 pending -1 unknown 0 No threat 1 Potential risk 2 Malicious |
| | process_trust | INTEGER | Parent process trust from Carbon Black File Reputation of the file associated with the event. Pending means that file lookup was not yet performed but will be. (Conditional) -2 pending -1 unknown 0-10 Trust value |
| | process_threat | INTEGER | Parent process threat from Carbon Black File Reputation of the file associated with the event. Pending means that file lookup was not yet performed but will be. (Conditional) -2 pending -1 unknown 0 No threat 1 Potential risk 2 Malicious |
| ✦ | process_hash | CHAR (64) | Hash of the process associated with the event |
| ✦ | command_line | NVARCHAR (1024) | Command line in the event description. Command lines may include proprietary information (e.g., passwords), and so their inclusion in events is optional. (Conditional) |
| ✦ | unified_source | NVARCHAR (256) | In a Unified Management environment, the server that initiated an action. (Conditional) |
| ✦ New or changed for v8.0.0. | | | |

Live Inventory SDK

App Control includes public views into its “live inventory” database of files, assets and events. You can create your own reporting and data analysis solutions through the use of these public views. The schema for these public views is **bit9_public** and the view for events is **ExEvents**.

Please refer to “Appendix A. Live Inventory SDK: Database Views” in the *Carbon Black App Control User Guide* or online Help in the App Control Console for more details.

Event Output for External Analytics

An App Control Server can be configured to send data, including App Control event data, to external data analytics tools, such as Splunk. Data exported for external analytical tools is in JSON format. It includes the field name with each value, making it easier both to view the raw output and to parse it later without creating indexing dependencies.

Please refer to “Exporting Data for External Analysis” in the *Using App Control* guide or online Help in the App Control Console for more details.

Archive Files

You can choose to have the App Control Server export a daily archive of events to a GZIP-compressed CSV file named in the format `yyyy-mm-dd.csv.gz`. To enable this feature, go to the Events tab of the System Configuration page, click Edit, check the Archive Events Enabled box, and click Update. The location of these archive files is in a subfolder of the server installation directory, by default:

```
C:\Program Files (x86)\Bit9\Parity Server\archivelogs\
```

The following table describes the columns in these archive files.

Table 13. Event Archive CSV File Columns

| | Archive CSV column | Note |
|---|---------------------|---|
| | TIMESTAMP | Time event occurred on agent (in UTC) |
| | RECEIVEDTIMESTAMP | Time event was received on server (in UTC) |
| | EVENTTYPE | Event type name |
| | EVENTSUBTYPE | Event subtype name |
| | COMPUTER | Event source (computer name or 'System') |
| + | COMPUTER_ID | Event source (Unique numeric ID, 0 for 'system') |
| | PLATFORM | Platform of the computer associated with the event |
| | IP_ADDRESS | IP address associated with the event |
| | MESSAGE | Event description |
| | POLICY | Name of the policy associated with the event |
| | FILENAME | Full file path |
| | PROCESSNAME | Name of the process associated with the event |
| | HASH | File hash |
| | HASH_TYPE | Type of the file hash (2 = SHA1, 3=MD5, 5=Sha256, 6=MSI) |
| | INSTALLER_HASH | Installer hash |
| | INSTALLER_HASH_TYPE | Type of the installer hash (2 = SHA1, 3=MD5, 5=Sha256, 6=MSI) |
| | RULE_NAME | Name of the rule associated with the event (if any) |
| | RULE_TYPE | Rule type of the rule associated with the event |
| | BAN_NAME | For blocked file events, the name of the ban that blocked the file action; some bans are unnamed |
| | UPDATER_NAME | Name of the Updater associated with the event (if any) |
| | SEVERITY | Event severity Change Notes: This column was labeled “priority” in pre-7.2.1 releases |
| | USERNAME | Name of user associated with the event |
| | PROCESS_HASH | Hash of the process associated with the event |
| | PROCESS_HASH_TYPE | Hash type of the process associated with the event |
| | ROOT_NAME | Installer name associated with the event |
| | GLOBAL_STATE | Global state of the file associated with the event (Approved/Unapproved) |
| | INDICATOR_NAME | Name of the threat indicator associated with the event (if any) |
| | FILE_TRUST | File trust from Carbon Black File Reputation of the file associated with the event. Pending means that file lookup was not yet performed but will be. |

| | Archive CSV column | Note |
|---|----------------------------|--|
| | | (Conditional) -2 pending -1 unknown 0-10 Trust value |
| | FILE_THREAT | File threat from Carbon Black File Reputation of the file associated with the event. Pending means that file lookup was not yet performed but will be. (Conditional) -2 pending -1 unknown 0 No threat 1 Potential risk 2 Malicious |
| | PROCESS_TRUST | Parent process trust from Carbon Black File Reputation of the file associated with the event. Pending means that file lookup was not yet performed but will be. (Conditional) -2 pending -1 unknown 0-10 Trust value |
| | PROCESS_THREAT | Parent process threat from Carbon Black File Reputation of the file associated with the event. Pending implies that file lookup was not yet performed but will be. (Conditional) -2 pending -1 unknown 0 No threat 1 Potential risk 2 Malicious |
| | USAGE_COUNTER | Prevalence of file related to this event |
| | PROCESS_USAGE_COUNTER | Prevalence of parent process related to this event |
| + | PROCESS_KEY | Unique proprietary key identifying the instance of the process on a specific computer |
| + | COMMAND_LINE | Command line in the event description. Command lines may include proprietary information (e.g., passwords), and so their inclusion in events is optional. |
| + | UNIFIED_SOURCE | In a Unified Management environment, the server that initiated an action. |
| + | New or changed for v8.0.0. | |

Contacting VMware Carbon Black Support

Please view our Customer Support Guide on the User Exchange for more information about Technical Support:

<https://community.carbonblack.com/t5/Support-Zone/Guide-to-Carbon-Black-Customer-Support/tap/34324>

For your convenience, support for App Control 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, App Control 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 |