Bit9 Security Platform 7.2.2

Events Integration Guide

Version 7.2.2.1119
Patch 2
29 April 2016

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

Contents

Introduction

This document describes the events generated, tracked, stored, and accessible through the Bit9 Security Platform.

Section 1, Event Specification, details the content, structure and purpose of these events for the benefit of integrators interested in using them outside of the Bit9 environment. This section includes a comprehensive list of event subtypes and their descriptions.

Section 2, Access to Bit9 Event Data, describes the ways you can access Bit9 event data outside of the Bit9 Console user interface. For supported syslog formats, this section describes how event data is mapped.

Bit9 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 the Bit9 Security Platform
- what Bit9 Server configuration changes have been made
- conditions requiring action (e.g., low disk space or database issues)

For computers running the Bit9 Agent, events can provide information such as:

- file executions that have been blocked due to security rules
- malicious files found by Bit9 or connected third-party security devices
- new devices found

Bit9 Platform v7.2.1 introduced the Bit9 API, which allows programmers who want to write code to interact with Bit9 Platform using custom scripts or from other applications. As with actions performed through the Bit9 Console, Bit9 API activity creates an audit trail. The appropriate API user taking the action is referenced in 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.*
- A Bit9 Security Platform 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 the Bit9 Security Platform features associated with these events, see the *Using the Bit9 Security Platform* guide, which is available as a PDF file or in online help on the Bit9 Console.

Note: The main table of event types and subtypes in Table 3 describes events as they appear in current versions of Bit9 Security Platform v7.2.2.

Section 1: Event Specification

The key elements of the Bit9 event specification are: the **event fields**, that is, the different types of information available in a single event; and the list of unique **event type/subtype** combinations, shown in Table 3 beginning on page 10.

Event Fields

This section describes the fields that can be in a Bit9 event. Those shown as "required" can be expected to be present in each Bit9 event. Other fields are present only for certain events or under certain conditions.

Timestamp (required)

All event timestamps are stored in UTC in the Bit9 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 Bit9 Console, timestamps are displayed according to the time zone setting selected on the **System Configuration > General** page.

The timestamp for an event corresponds to the date/time when the *Bit9 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 Bit9 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, other event output from Bit9 may also include a *received* timestamp that shows the time the Bit9 Server received an event.

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 1 shows the public event types.

Table 1. Bit9 Event Types

Event Type	Description
Computer Management	Events related to changes to Computer assets managed by the Bit9 Server or specific to a Bit9 Agent. For example: - 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 sensor status"
Discovery	Reporting events related to the discovery or existence of new assets or new actions. For example: - 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 Bit9 Software Reputation Service, Bit9'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	Events related to the management of non-user, non-computer and non-policy assets. Specifically, this includes events related to meters, alerts, baseline drift reports, snapshots, and event rules. For example, "Alert triggered", "Baseline drift report generated"
Policy Enforcement	Events related to the enforcement of any policy or rule on the Bit9 Agent. For example: - 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)" **Note:** This does *not* include the creation or management of policies. Those events are included under the Policy Management type.
Policy Management	Events related to the management (creation, modification, deletion) of any policy or rule. For example: - 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"

Event Type	Description
	- Memory rule events like “Memory rule modified”
Server Management	Events related to the configuration and administration of the Bit9 Server and database. For example: - “Server shutdown”, “License added”, “Server backup stopped”, “Database error” and “Bit9 Software Reputation Service connection lost”
Session Management	Events related to the login activity and management of Bit9 Console users. For example: - Management events like “Console user created” - Login activity like “Console user login” and “Console user logout” **Note:** Bit9 Console is the web-based user interface to the Bit9 Server through which all standard Bit9 Security Platform administration takes place.

Subtype (required)

The subtype uniquely corresponds to one (and only one) event type. Subtypes generally map closely to real world use cases and/or Bit9 product functionality. The full list of subtypes is provided in Table 3.

Severity (required)

Each Bit9 event has one of five different severity values. Table 2 shows the severity values listed in order of ascending importance. Note that prior to v7.2.1, this field was called “Priority”.

Table 2. Bit9 Event Severities

Priority	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 Bit9 Support
2 - Critical	Critical condition that requires immediate investigation or action

Description (required)

The description field is an English-language text description of the event. Often, the description will contain redundant information from 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.

Source (required)

There are two possible values for Source: “System” (indicating the Bit9 Server or a server component) or a computer name (indicating the event came from a Bit9 Agent on the named computer).

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 Bit9 Agent generated events. This is the IP address of the agent at the time of the event, not the current IP address of the agent.

Events generated by the Bit9 Console report the IP address of the machine on which the user is accessing the Bit9 Console. For example, "Console user login" and "File approval created" events contain the IP address of the computer on which a user performed those actions.

Most events generated by the Bit9 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 computer (Source) at the time of the event, or the Console User in the case of events generated from the Bit9 Console. There are cases in which an event cannot be attributed to either a console or a logged in user on an agent system, and the results of this condition vary:

- 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 occur under the context of the Bit9 Agent 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, the Bit9 Platform 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 – Bit9 will use the special string "<unknown>" for User.

File Hash, File Name, File Path, File Trust, and File Threat

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 value. The File Path does *not* end with a trailing slash.

If Bit9 Software Reputation Service 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 Name, Process Path, Process Key, Process Trust, and Process Threat

Several Process fields are used within events generated by the Bit9 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.

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 Bit9 Software Reputation Service 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 that identifies 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 archive events.

Installer, Root Hash

Installer and Root Hash are used within some events generated by the Bit9 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* generates the file *myapp.exe.* When *myapp.exe* is first written on a Bit9 Agent computer, 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 s*etup123.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 Bit9 Agent. It contains the name of the Bit9 security policy in effect on the agent at the time of the event.

Events Table

Table 3 lists all events types and their unique subtypes in the Bit9 Security Platform v7.2.2. New or changed events are shown with the following legend:

●	New for v7.2.2; type and subtype shown in bold	♦	New for v7.0.1
○	Changed for v7.2.2 (e.g., type, subtype, priority, description, triggering condition); type and subtype shown in bold	◊	Changed for v7.0.1
♣	New for v7.2.1; type and subtype shown in bold	▲	New for v7.0.0
♧	Changed for v7.2.1 (e.g., type, subtype, priority, description, triggering condition); type and subtype shown in bold	Δ	Changed for v7.0.0
★	New for v7.2.0	x	Deleted from v7.0.0
☆	Changed for v7.2.0		

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, "Laptop-5", for example, the Description column in this table shows "$computer$". Variables that use parameters from the Bit9 Platform, where these parameters are not commonly known objects outside of the Bit9 context, are shown in the format "$param1$", "$param2$", etc. You can view the actual event output from Bit9 or view the Events page through Bit9 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 appear as follows 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 pre-7.2.0 version of Bit9, note the following changes that affect multiple events:

- Bit9 Security Platform v7.2.2 supports non-Windows agents, so path syntax in agent-related event descriptions varies by operating system.
- Event subtypes related to *file-signing* certificates were added to Bit9 Parity v7.0.1. *Communications* certificate events already in Bit9 Parity were renamed to begin with "SSL" (e.g., "Certificate expiring" became "SSL certificate expiring"). These changes are noted for each affected subtype.
- Several product name changes beginning with v7.2.0 have affected certain event subtypes and descriptions:
  - Parity Server is now Bit9 Server
  - Parity Agent is now Bit9 Agent
  - Parity Console is now Bit9 Console
  - Parity Knowledge Service is now Bit9 Software Reputation Service
- Numerous other changes, including some user interface names, were made during the 7.0.0/7.0.1 product cycle.
- Beginning with 7.2.1, what was labeled "Priority" is now "Severity".

Table 3. Bit9 Security Platform 7.2.2 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 '$param2$'. 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'.
	Computer Management	Agent database error	432	Error	Bit9 Agent had to restore its primary database cache. Bit9 Agent had to rebuild its primary database cache and now has to re-initialize. Bit9 Agent detected a cache integrity problem. Unknown error initializing database pool. Bit9 Agent had to restore its primary database cache. Bit9 Agent had to rebuild its primary database cache and now has to re-initialize. Bit9 Agent failed to upgrade its database. Bit9 Agent failed to connect to its cache database. Bit9 Agent failed to read config list from file. Bit9 Agent failed cache verification.
	Computer Management	Agent deleted events	414	Notice	Computer '$computer$' deleted $param1$ events. Param1 is a numeric value.
∆	Computer Management	Agent Enforcement Level changed	407	Notice	Computer '$computer$' changed Enforcement Level from '$param1$' to '$param2$'. Parameters 1 and 2 are one of the Enforcement Levels or Local Approval. ***Change Notes:*** *In 6.0.x, subtype was "Agent SecCon changed" and message referred to "SecCon".*
	Computer Management	Agent error	431	Error	Unsupported kernel [$kernelversion$] running. Agent will not track files. Bit9 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: $logoFilePath$.

● New for v7.2.2 ○ Changed for v7.2.2 ♣ New for v7.2.1 ♧ Changed for v7.2.1 ★ New for v7.2.0 ☆ Changed for v7.2.0
♦ New for v7.0.1 ◊ Changed for v7.0.1 ▲ New for v7.0.0 ∆ Changed for v7.0.0 X Deleted from v7.0.0

	Type	Subtype	ID No.	Severity	Example Descriptions/Comments
▲	Computer Management	Agent health check	447	Info/ Error/ Warning	Bit9 Agent is healthy. Options[$param1$]. Bit9 Agent failed a health check. ErrorsFound[$param2$] Options[$param1$] Bit9 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
★	Computer Management	Agent health check request	457	Info	User '$userName$' requested health check for computer '$computer$'.
	Computer Management	Agent policy changed	406	Notice	Computer '$computer$' changed policies from '$param1$' to '$param2$'.
	Computer Management	Agent policy updated	408	Info	Computer '$computer$' updated policy from version '$param1$' to '$param2$'.
	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	Bit9 Agent has started, version $param1$.
	Computer Management	Agent shutdown	404	Info	Bit9 Agent was stopped because of a system shutdown.
	Computer Management	Agent synchronization finished	411	Info	Computer '$computer$' finished resynchronizing its local state with the Bit9 Server. (Reason: '$param1$') 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'
	Computer Management	Agent synchronization requested	418	Info	User '$username$' has requested resynchronization of computer '$computer$' with the Bit9 Server.
○	**Computer Management**	**Agent synchronization started**	410	Info	Computer '$computer$' started resynchronizing its local state with the Bit9 Server (Reason: $param2$). ***Change Notes:*** *Reason field added for 7.2.2.*
	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	Bit9 Server scheduled an auto resync on '$computer$' because agent appears to have gone back in time ($param1$/$param2$). 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 Bit9 Support.
☆	Computer Management	Cache check complete	416	Info	Cache consistency check stopped Level [$param1$] $param2$ Param1 is the cache consistency level. Param2 is a series of values for diagnosis of what was done during the check; it also indicates whether the check ran to completion ("Successful[1]") or stopped before completion ("Successful[0]"). ***Change Notes:*** *The description changed in 7.2.0.*
	Computer Management	Cache check error	417	Warning	Cache consistency error number '$param1$', file '$param2$'
Δ	Computer Management	Cache check start	426	Info	Cache consistency check at level '$param1$', flags '$param2$' started. ***Change Notes:*** *The message in 7.0.0 and later adds a flags parameter.*

● New for v7.2.2 ○ Changed for v7.2.2 ♣ New for v7.2.1 ♧ Changed for v7.2.1 ★ New for v7.2.0 ☆ Changed for v7.2.0
♦ New for v7.0.1 ◊ Changed for v7.0.1 ▲ New for v7.0.0 Δ Changed for v7.0.0 X Deleted from v7.0.0

	Type	Subtype	ID No.	Severity	Example Descriptions/Comments
★	Computer Management	Cache consistency check request	453	Info	User '$userName$' requested a cache consistency check Level[$param1$] Options[$param2$] for computer '$computer$'] Param1 is the consistency check level chosen by the user and param2 indicates any option checkboxes chosen, such as "Full scan of new files".
★	Computer Management	Carbon Black sensor status	458	Info	Carbon Black Sensor Version '$param1' installed and '$param2'. Carbon Black Sensor is not installed. ***Notes:*** *param1 is the Carbon Black sensor version; param2 is the sensor state (e.g., 'Running').*
	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 '$username$'. 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 '$username$'. ***Change Notes:*** *All but first description message were new for 7.0.0.*
▲	Computer Management	Computer Reboot Request	441	Info	User '$username$' requested reboot of computer '$computer$'.
	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.
	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 deletion request	454	Info	User '$userName$' requested deletion of diagnostic files from computer '$computer$.
	Computer Management	File process error	423	Error	Agent on computer '$computer$' is unable to process required update '$param1$' from Bit9 Server.
	Computer Management	File receive error	422	Warning	Agent on computer '$computer$' is unable to download required update '$param1$' from Bit9 Server.

● New for v7.2.2 ○ Changed for v7.2.2 ♣ New for v7.2.1 ♧ Changed for v7.2.1 ★ New for v7.2.0 ☆ Changed for v7.2.0
♦ New for v7.0.1 ◊ Changed for v7.0.1 ▲ New for v7.0.0 ∆ Changed for v7.0.0 X Deleted from v7.0.0

	Type	Subtype	ID No.	Severity	Example Descriptions/Comments
▲	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$'. ***Change Notes:*** *New event for 7.0.0 Patch 10 and 7.0.1 Patch 7.*
▲	Computer Management	File upload error	440	Error	Upload of file [$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 '$ruleName$'. ***Change Notes:*** *In7.0.0 Patch 10 and 7.0.1 Patch 7, message options were expanded to include uploads triggered by event rules.*
	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. ***Change Notes:*** *In 7.2.2, the description was changed to indicate "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 '$username$'.
★	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.
▲	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 Bit9 (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.
	Computer Management	Tamper Protection changed	428	Warning	User '$username$' has disabled Tamper Protection on computer '$computer$'.
▲	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 '$computer$'.

● New for v7.2.2 ○ Changed for v7.2.2 ♣ New for v7.2.1 ♧ Changed for v7.2.1 ★ New for v7.2.0 ☆ Changed for v7.2.0
♦ New for v7.0.1 ◊ Changed for v7.0.1 ▲ New for v7.0.0 Δ Changed for v7.0.0 X Deleted from v7.0.0

	Type	Subtype	ID No.	Severity	Example Descriptions/Comments
○ ∆	**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. ***Change Notes:*** *In 6.0.x, the subtype was "Temporary SecCon override" and the message referred to "SecCon" instead of "Enforcement Level". In 7.2.2, the description was changed and a parameter for the length of time in override was added.*
∆	Computer Management	Temporary Enforcement Level restore	420	Notice	Computer '$computer$' has been restored to Enforcement Level $param1$. ***Change Notes:*** *In 6.0.x, the subtype was "Temporary SecCon restore" and the message referred to "SecCon" instead of "Enforcement Level".*
	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 $param2$ minute(s).
	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 '$filePathAndName$' with hash [$hash$].
♦	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 added	1013	Info	Certificate '$param1$' was added by user '$username$'.
	Discovery	Certificate revocation	1011	Warning	Computer $computer$ detected revocation of certificate '$param1$' on file '$filePathAndName$ Error: $param2$ **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. ***Change Notes:*** *New in 7.0.0 Patch 10 and 7.0.1 Patch 7.*
	Discovery	File group created	1001	Info	Installation group was created for the file '$filePathAndName$' with hash [$hash$].
	Discovery	First execution on network	1007	Info	File '$filePathAndName$' with hash [$hash$] was executed for the first time.

● New for v7.2.2 ○ Changed for v7.2.2 ♣ New for v7.2.1 ♧ Changed for v7.2.1 ★ New for v7.2.0 ☆ Changed for v7.2.0
♦ New for v7.0.1 ◊ Changed for v7.0.1 ▲ New for v7.0.0 ∆ Changed for v7.0.0 X Deleted from v7.0.0

	Type	Subtype	ID No.	Severity	Example Descriptions/Comments
Δ ♧	Discovery	Malicious file detected	1201	Warning	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 Bit9 Software Reputation Service as a malicious file. ***Note:*** *External providers are Check Point, FireEye, Palo Alto Networks or Microsoft. Other providers might be added through the Bit9 API.* ***Change Notes:*** *In 6.0.x, Type was "Parity Knowledge". Descriptions changed in 7.0.0 Patch 10 and 7.0.1 Patch 7 to account for external notifications. In 7.2.1, Microsoft was added as a provider.*
♦	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 '$param2$'. Interactive user at the time: '$username$'.
	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.
Δ	Discovery	New unapproved file to computer	1003	Notice	Computer $computer$ discovered new file '$filePathAndName$' with hash [$hash$]. ***Change Notes:*** *In 6.0.x, the subtype was "New pending file to computer".*
Δ ♧	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 Bit9 Software Reputation Service as a potential risk. ***Note:*** *Standard external providers are Check Point, FireEye, Palo Alto Networks or Microsoft. Other providers might be added through the Bit9 API.* ***Change Notes:*** *In 6.0.x, Type was "Parity Knowledge". Descriptions changed in 7.0.0 Patch 10 and 7.0.1 Patch 7 to account for external notifications. In 7.2.1, Microsoft was added as a provider.*
♣	Discovery	Service created	1015	Info	'$computer$' detected the creation of a new service: $servicename$. ***Change Notes:*** *Added to 7.2.1 Patch 7.*
♣	Discovery	Service deleted	1016	Info	'$computer$' detected the deletion of a service: $servicename$. ***Change Notes:*** *Added to 7.2.1 Patch 7.*
●	**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 '$username$'.

● New for v7.2.2 ○ Changed for v7.2.2 ♣ New for v7.2.1 ♧ Changed for v7.2.1 ★ New for v7.2.0 ☆ Changed for v7.2.0
♦ New for v7.0.1 ◊ Changed for v7.0.1 ▲ New for v7.0.0 Δ Changed for v7.0.0 X Deleted from v7.0.0

	Type	Subtype	ID No.	Severity	Example Descriptions/Comments
♧	**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. ***Change Notes:*** *Previously,* ***Notice*** *was the severity for all alerts. In 7.2.1, it was changed to:* ***Critical*** *for High priority alerts;* ***Error*** *for Medium priority alerts;* ***Warning*** *for Low priority alerts.*
	General Management	Baseline drift report created	1106	Info	Baseline drift report '$param1$' has been created by '$userName$'.
	General Management	Baseline drift report deleted	1108	Info	Baseline drift report '$reportname1$' has been deleted by '$userName$'.
	General Management	Baseline drift report generated	1109	Info	Baseline drift report '$reportname$' has been generated.
	General Management	Baseline drift report generation is slow	1113	Warning	Drift report $reportname$ 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.*
	General Management	Baseline drift report modified	1107	Info	Baseline drift report '$reportname$' has been modified by '$userName$'.
▲	General Management	Event rule created	1114	Info	Event rule '$ruleName$' has been created by '$userName$'. ***Change Notes:*** *New in 7.0.0 Patch 10 and 7.0.1 Patch 7.*
▲	General Management	Event rule deleted	1116	Info	Event rule '$ruleName$' has been deleted by '$userName$'. ***Change Notes:*** *New in 7.0.0 Patch 10 and 7.0.1 Patch 7.*
▲ ☆	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 Notes:*** *New subtype in 7.0.0 P10 and 7.0.1 P7. New conditions two and three for 7.2.0.*
	General Management	Meter created	632	Info	Meter '$param1$' 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 '$param1$' was deleted by '$username$'. ***Note:*** *Type was incorrectly identified as Policy Management in previous editions of this document.*
	General Management	Meter modified	634	Info	Meter '$param1$' was modified by '$username$'. ***Note:*** *Type was incorrectly identified as Policy Management in previous editions of this document.*
	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$'.
	Policy Enforcement	Access block (memory rule)	830	Notice	Access to process '$filePathAndName$' was restricted - Requested[$param1] Restricted[$param2$]
	Policy Enforcement	Access prompt (memory rule)	831	Info	Access to process '$filePathAndName$' was granted because of a memory rule prompt response.
♣	Policy Enforcement	Banned Process Discovered	847	Warning	The Bit9 Agent discovered a banned process '$pathname$$pathSeparator$$filename$' [$hash$] that ran during system startup. $param1$

● New for v7.2.2 ○ Changed for v7.2.2 ♣ New for v7.2.1 ♧ Changed for v7.2.1 ★ New for v7.2.0 ☆ Changed for v7.2.0
♦ New for v7.0.1 ◊ Changed for v7.0.1 ▲ New for v7.0.0 Δ Changed for v7.0.0 X Deleted from v7.0.0

	Type	Subtype	ID No.	Severity	Example Descriptions/Comments
★	Policy Enforcement	Carbon Black watchlist	842	Notice	***If Process watchlist and file is known to Bit9:*** Carbon Black process watchlist '$ruleName$' hit for process '$process$' [$hash$] on computer '$computer$'. Carbon Black watchlist '$watchlist$' detected file '$filePathAndName$' [$filehash$] on computer '$computer$'. ***If Process watchlist and file is unknown to Bit9:*** Carbon Black process watchlist '$ruleName$' hit for unknown process '$process$' [$processhash$] on computer '$computer$'. Carbon Black watchlist '$watchlist$' detected unknown file '$filePathAndName$' [$hash$] on computer '$computer$'. ***If Binary watchlist and file is known to Bit9:*** Carbon Black binary watchlist '$ruleName$' detected file '$filePathAndName$' [$filehash$]. ***If Binary watchlist and file is unknown to Bit9:*** Carbon Black binary watchlist '$ruleName$' detected unknown file '$filePathAndName$' [$filehash$].
♣	Policy Enforcement	Execution allowed (file loaded before kernel)	843	Warning	The $param1$ file '$pathname$$pathSeparator$$filename$' [$hash$] executed before the Bit9 Agent was running. $param2$
♣	Policy Enforcement	Execution allowed (file loaded before service)	844	Warning	The $param1$ file '$pathname$$pathSeparator$$filename$' [$hash$] executed before the Bit9 Agent was enforcing. $param2$
	Policy Enforcement	Execution allowed (inactive)	841	Warning	Execution of file '$filePathAndName$' [$hash$] would have blocked if Bit9 Agent was active.
♣	Policy Enforcement	Execution allowed (New file discovered on startup)	845	Warning	The newly discovered file '$pathname$$pathSeparator$$filename$' [$hash$] was executing when the Bit9 Agent started. $param1$
∆	Policy Enforcement	Execution allowed (trusted user)	815	Notice	Execution of unapproved file '$filePathAndName$' with hash [$hash$] was allowed because of Trusted User '$username$'. ***Change Notes:*** *In 6.0.x, the message said "Execution of pending file…".*
♣	Policy Enforcement	Execution allowed (Unanalyzed file loaded before service)	846	Warning	The file '$pathname$$pathSeparator$$filename$' executed before the Bit9 Agent started. The file was removed before the Bit9 Agent could analyze it. $param2$
	Policy Enforcement	Execution block (banned file)	802	Notice	File '$filePathAndName$' with hash [$hash$] was blocked because it was banned.
☆	Policy Enforcement	Execution block (custom rule)	806	Notice	File '$filePathAndName$' with hash [$hash$] was blocked because of a custom rule. Process '$process$' was terminated due to the banned image '$filePathAndName$' [$hash$]. ***Change Notes:*** *The process termination case was added for v7.2.0.*
○	**Policy Enforcement**	**Execution block (network file)**	805	Notice	The file '$filePathAndName$' [$hash$] was blocked because it was located on a remote drive. ***Change Notes:*** *The description was slightly modified for 7.2.2.*
	Policy Enforcement	Execution block (prompt timeout)	839	Notice	File '$filePathAndName$' with hash [$hash$] was blocked from execution because.
	Policy Enforcement	Execution block (removable media)	819	Notice	File '$filePathAndName$' with hash [$hash$] was blocked from execution because it was on removable media.
	Policy Enforcement	Execution block (still analyzing)	804	Info	File '$filePathAndName$' was blocked because Bit9 Agent did not have time to analyze it.

● New for v7.2.2 ○ Changed for v7.2.2 ♣ New for v7.2.1 ♧ Changed for v7.2.1 ★ New for v7.2.0 ☆ Changed for v7.2.0
♦ New for v7.0.1 ◊ Changed for v7.0.1 ▲ New for v7.0.0 ∆ Changed for v7.0.0 X Deleted from v7.0.0

	Type	Subtype	ID No.	Severity	Example Descriptions/Comments
Δ	Policy Enforcement	Execution block (unapproved file)	801	Notice	File '$filePathAndName$' with hash [$hash$] was blocked because it was unapproved. ***Change Notes:*** *In 6.0.x, subtype was "Execution block (pending file)" and message referred to a "pending" file.*
	Policy Enforcement	Execution prompt (custom rule)	818	Info	File '$filePathAndName$' [$hash$] was executed because of a custom rule prompt response.
Δ	Policy Enforcement	Execution prompt (unapproved file)	814	Info	File '$filePathAndName$' with hash [$hash$] was approved because of user response. ***Change Notes:*** *This was "Execution prompt (block and ask)" in v6.0.2.*
	Policy Enforcement	Execution prompt allowed (unapproved file)	838	Info	File '$filePathAndName$' [$hash$] was approved because of user response.
	Policy Enforcement	Execution prompt block (unapproved file)	837	Info	File '$filePathAndName$' [$hash$] was blocked because of user response.
	Policy Enforcement	File access error	825	Warning	Unable to access the file '$filePathAndName$'.
	Policy Enforcement	File approved (cache consistency)	835	Info	File '$filePathAndName$' with hash [$hash$] was approved because of a cache consistency scan.
	Policy Enforcement	File approved (custom rule)	833	Info	File '$filePathAndName$' with hash [$hash$] was approved because of a custom rule.
	Policy Enforcement	File approved (local approval)	813	Info	File '$filePathAndName$' with hash [$hash$] was locally approved.
♦ ☆	Policy Enforcement	File approved (publisher)	812	Info	File '$filePathAndName$' [$hash$] was approved by Publisher '$publisherName$'. ***Change Notes:*** *Prior to 7.2.0 the type was documented incorrectly as "Policy Management".*
▲	Policy Enforcement	File approved (reputation)	840	Info	File '$filePathAndName$' [$hash$] was approved by reputation.
	Policy Enforcement	File approved (system update)	836	Info	File '$filePathAndName$' with hash [$hash$] was approved due to Windows Update. ***Note****: Applies to the package/root files from Windows Update, not files installed from them.*
	Policy Enforcement	File approved (trusted user)	810	Info	File '$filePathAndName$' with hash [$hash$] was approved by Trusted User '$username$'.
	Policy Enforcement	File approved (updater)	811	Info	File '$filePathAndName$' with hash [$hash$] was approved by an Updater.
	Policy Enforcement	File approved (version resource)	834	Info	File '$filePathAndName$' with hash [$hash$] was approved because of version resource.
	Policy Enforcement	Metered execution	816	Notice	Metered file '$filePathAndName$' with hash [$hash$] was executed by the user '$username$'.
●	**Policy Enforcement**	**Prompt canceled**	849	Warning	Prompt '$filePathAndName$' [$hash$] prompt is canceled ($param1$). Param1 shows the reason a notifier prompt was cancelled. It can be one of the following: • 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). • SubsequentBlock – 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). • AgentShutdown – System or daemon shutdown while the prompt was still outstanding. File will be blocked in this case. • PingTimeout – Agent was unable to communicate with notifier and canceled the prompt. This is an error case and should be rare. ***Platform Note:*** *This event only occurs for Mac OS X and Linux agents.*

● New for v7.2.2 ○ Changed for v7.2.2 ♣ New for v7.2.1 ♧ Changed for v7.2.1 ★ New for v7.2.0 ☆ Changed for v7.2.0
♦ New for v7.0.1 ◊ Changed for v7.0.1 ▲ New for v7.0.0 Δ Changed for v7.0.0 X Deleted from v7.0.0

	Type	Subtype	ID No.	Severity	Example Descriptions/Comments
	Policy Enforcement	Read block (removable media)	821	Notice	Read access to file '$filePathAndName$' with hash [$hash$] was blocked because it was on removable media.
	Policy Enforcement	Report access (memory rule)	829	Info	Access to process '$filePathAndName$' was granted – Requested[$param1] ***Note:*** *Param1 is a hex number indicating the Windows code of the permissions requested.*
☆	Policy Enforcement	Report execution (custom rule)	807	Notice	File '$filePathAndName$' with hash [$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 Notes:*** *The process termination cases were added in v7.2.0.*
	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.
	Policy Enforcement	Report write (custom rule)	809	Info	File '$filePathAndName$' was modified or deleted.
	Policy Enforcement	Report write (registry rule)	826	Info	Registry '$filePathAndName$' was modified or deleted.
	Policy Enforcement	Report write (removable media)	823	Info	File '$filePathAndName$' was modified or deleted on removable media.
∆	Policy Enforcement	Tamper Protection	832	Warning	Execution of '$filePathAndName$' by '$username$' was blocked because of tamper protection. Modification of '$filePathAndName$' by '$username$' was blocked because of tamper protection. 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 Notes:*** *The conditions triggering this event and the associated messages have changed between v6.0.2 and v.7.0.0.*
X	Policy Enforcement	Tamper Protection blocked	800	Warning	Bit9 Agent blocked access to the file '$filePathAndName$' by its Tamper Protection policy. ***Change Notes:*** *This subtype is was deleted in 7.0.0. The condition triggering it is now one of the conditions for the subtype Tamper Protection (832).*
♣	Policy Enforcement	Unapproved Process Discovered	848	Warning	The Bit9 Agent discovered an unapproved process '$pathname$$pathSeparator$$filename$' [$hash$] that ran during system startup. $param1$
	Policy Enforcement	Write block (custom rule)	808	Notice	Modification of file '$filePathAndName$' with hash [$hash$] was blocked because of a custom rule.
	Policy Enforcement	Write block (registry rule)	827	Notice	Modification of registry '$filePathAndName$' was blocked.
	Policy Enforcement	Write block (removable media)	820	Notice	Modification of file '$filePathAndName$' with hash [$hash$] was blocked because it was on removable media.

● New for v7.2.2 ○ Changed for v7.2.2 ♣ New for v7.2.1 ♧ Changed for v7.2.1 ★ New for v7.2.0 ☆ Changed for v7.2.0
♦ New for v7.0.1 ◊ Changed for v7.0.1 ▲ New for v7.0.0 ∆ Changed for v7.0.0 X Deleted from v7.0.0

	Type	Subtype	ID No.	Severity	Example Descriptions/Comments
	Policy Enforcement	Write prompt (custom rule)	817	Info	Registry '$filePathAndName$' was modified or deleted because of a registry rule user response. Modification of file '$filePathAndName$' [$hash$] was blocked because of a custom rule user response.
	Policy Enforcement	Write prompt (registry rule)	828	Info	Modification of registry '$filePathAndName$' was blocked because of a registry rule user response.
	Policy Management	AD rules changed	604	Notice	'$username$' created an AD rule for mapping $param1$ to the policy $policyName$.
	Policy Management	AD rules loaded	605	Info	Active Directory rules script with version $param1$ was loaded successfully.
▲	Policy Management	Approval Request Closed	646	Info	Approval Request was closed by user '$username$'.
▲	Policy Management	Approval Request Created	644	Info	Approval Request was created by user '$username$'.
▲	Policy Management	Approval Request Opened	645	Info	Approval Request was opened by user '$username$'.
♦ ☆	Policy Management	Certificate approval created	651	Info	Certificate $SubjectName$ was approved by $username$ for publisher $publisher$. ***Change Notes:*** *This event has not changed but prior to 7.2.0 was documented incorrectly as being in the "Policy Enforcement" type.*
♦ ☆	Policy Management	Certificate approval deleted	653	Info	Approval of certificate $SubjectName$ was deleted by '$username$' for publisher $publisher$. ***Change Notes:*** *This event has not changed but prior to 7.2.0 was documented incorrectly as being in the "Policy Enforcement" type.*
	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 $publisher$. ***Change Notes:*** *This event has not changed but prior to 7.2.0 was documented incorrectly as being in the "Policy Enforcement" type.*
○ ♦	**Policy Management**	**Certificate ban deleted**	656	Info	Ban of certificate $SubjectName$ was deleted by '$username$' for publisher $publisher$. ***Change Notes:*** *In 7.2.2, the description was slightly modified.*
★	Policy Management	Certificate ban modified	655	Info	Ban of certificate '$subjectName$' was modified by '$username$' for publisher '$param3$'.
♧	Policy Management	Custom rule created	638	Info	Custom rule '$ruleName$' was created by '$username$'. '$ruleName$' was imported by '$username'. ***Change Notes:*** *Rule imports were new in v7.2.1.*
	Policy Management	Custom rule deleted	640	Info	Custom rule '$ruleName$' was deleted by '$username$'.
♧	Policy Management	Custom rule modified	639	Info	Custom rule '$ruleName$' was modified by '$username$'. '$ruleName$' was imported by '$username'. ***Change Notes:*** *Rule imports were new in v7.2.1.*
○ ∆	**Policy Management**	**Device rule created**	641	Info	Device rule for 'ruleName' with id 'ruleID' was created by '$username$'. ***Change Notes:*** *In 6.0.x, this was "Device approval created". In 7.2.2, the description was modified and ruleID was added.*
∆	Policy Management	Device rule deleted	642	Info	Rule for device '$deviceName$' was removed by '$username$'. ***Change Notes:*** *In 6.0.x, this was "Device approval removed".*
▲	Policy Management	Device rule modified	643	Info	Rule for device '$deviceName$' was modified by '$username$'.

● New for v7.2.2 ○ Changed for v7.2.2 ♧ New for v7.2.1 ♧ Changed for v7.2.1 ★ New for v7.2.0 ☆ Changed for v7.2.0
♦ New for v7.0.1 ◊ Changed for v7.0.1 ▲ New for v7.0.0 ∆ Changed for v7.0.0 X Deleted from v7.0.0

	Type	Subtype	ID No.	Severity	Example Descriptions/Comments
	Policy Management	File approval created	627	Info	Approval '$ruleName$' for hash [$hash$] was created by '$username$'. ***Note:*** *In v6.0 this event/subevent was also used when user marked or unmarked a file as an installer.*
	Policy Management	File approval deleted	629	Info	Approval '$ruleName$' for hash [$hash$] was deleted by '$username$'.
	Policy Management	File approval modified	628	Info	Approval '$ruleName$' 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 '$param1$' was created by '$username$'.
	Policy Management	File ban deleted	637	Info	Ban '$param1$' was deleted by '$username$'.
	Policy Management	File ban modified	636	Info	Ban '$param1$' was modified by '$username$'.
	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 '$username$'.
Δ	Policy Management	File remove local approval	625	Info	File '$filePathAndName$' [$hash$] was changed to unapproved on computer $computer$ by '$userName$'. ***Change Notes:*** *In 6.0.x, description message referred to a "pending" file.*
	Policy Management	Install package created	603	Notice	An $param1$ install package $policyName$.msi was created by '$username$'. ***Note:*** *Param1 is either empty or "automatic" for packages that allow automatic AD policy assignment.*
▲	Policy Management	Justification created	650	Info	Justification Request was created by user '$username$'.
♧	Policy Management	Memory rule created	129	Info	Memory rule '$ruleName$' created by '$username$'. '$ruleName$' was imported by '$username'. ***Change Notes:*** *Rule imports were new in v7.2.1.*
	Policy Management	Memory rule deleted	131	Info	Memory rule '$ruleName$' deleted by '$username$'.
♧	Policy Management	Memory rule modified	130	Info	Memory rule '$ruleName$' modified by '$username$'. '$ruleName$' was imported by '$username'. ***Change Notes:*** *Rule imports were new in v7.2.1.*
▲	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 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 '$userName$'.
	Policy Management	Policy file tracking enabled	607	Notice	File tracking has been enabled for policy '$policyName$' by '$userName$'.

● New for v7.2.2 ○ Changed for v7.2.2 ♣ New for v7.2.1 ♧ Changed for v7.2.1 ★ New for v7.2.0 ☆ Changed for v7.2.0
♦ New for v7.0.1 ◊ Changed for v7.0.1 ▲ New for v7.0.0 Δ Changed for v7.0.0 X Deleted from v7.0.0

	Type	Subtype	ID No.	Severity	Example Descriptions/Comments
	Policy Management	Policy modified	602	Info	Policy '$policyName$' was modified by '$username$'.
Δ	Policy Management	Process demoted	1006	Notice	Process $filePathAndName$ was demoted on the computer '$computer$'. New files written by this process will be unapproved. ***Change Notes**: In 6.0.x, the message said new files would be "pending". In the first builds of 7.0.0, the event type was "Discovery".*
	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 '$username$'. ***Change Notes**: In 7.2.2, the description was slightly modified.*
	Policy Management	Publisher modified	630	Info	Publisher '$publisherName$' was edited by '$username$'.
♧	Policy Management	Registry rule created	132	Info	Registry rule '$ruleName$' created by '$username$'. '$ruleName$' was imported by '$username'. ***Change Notes:** Rule imports were new in v7.2.1.*
	Policy Management	Registry rule deleted	134	Info	Registry rule '$ruleName$' deleted by '$username$'.
♧	Policy Management	Registry rule modified	133	Info	Registry rule '$ruleName$' modified by '$username$'. '$ruleName$' was imported by '$username'. ***Change Notes:** Rule imports were new in v7.2.1.*
	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 '$username$'.
▲	Policy Management	Script rule created	647	Info	Script rule '$ruleName$' was created by '$username$'.
▲	Policy Management	Script rule deleted	648	Info	Script rule '$ruleName$' was deleted by '$username$'.
▲	Policy Management	Script rule modified	649	Info	Script rule '$ruleName$' was modified by '$username$'.
	Policy Management	Trusted directory check	608	Info	Trusted directory '$pathName$' on computer '$computer$' is '$param2$'. ***Note:** Param2 is the result of the check (i.e., valid or invalid).*
	Policy Management	Trusted directory created	613	Info	Approval directory '$pathname$' added by '$username$'.
	Policy Management	Trusted directory deleted	615	Info	Approval directory '$pathname$' deleted by '$username$'.
	Policy Management	Trusted directory import	626	Info, Warning, Error	Trusted package '$param1$' from computer '$computer$' has been processed. ***Note:** Priority is **Info** for status imports; **Warning** for improperly signed or misidentified manifests; **Error** for all other cases.*
	Policy Management	Trusted directory modified	614	Info	Approval directory '$filePathAndName$' modified by '$username$'.

● New for v7.2.2 ○ Changed for v7.2.2 ♣ New for v7.2.1 ♧ Changed for v7.2.1 ★ New for v7.2.0 ☆ Changed for v7.2.0
♦ New for v7.0.1 ◊ Changed for v7.0.1 ▲ New for v7.0.0 Δ Changed for v7.0.0 X Deleted from v7.0.0

	Type	Subtype	ID No.	Severity	Example Descriptions/Comments
	Policy Management	Trusted directory scan	609	Info	Pre-approval scan started for '$filePathAndName$'. Approval ID: $param1$. Job ID: $param2$.
	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	Updater disabled	621	Info	Updater '$updaterName$' was disabled by '$username$'.
	Policy Management	Updater enabled	620	Info	Updater '$updaterName$' was enabled 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 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 previous versions.*
☆	Server Management	Bit9 Software Reputation Service connection lost	138	Warning	Bit9 Software Reputation Service connection lost: $reason$ ***Change Notes:*** *In pre-7.2.0 releases, the subtype referred to "Parity Knowledge Service".*
☆ Δ	Server Management	Bit9 Software Reputation Service connection restored	139	Notice	*Bit9 Software Reputation Service connection restored* ***Change Notes:*** *In 6.0.x, Priority was "Info" and message was less descriptive. Also, in pre-7.2.0 releases, the subtype referred to "Parity Knowledge Service".*
☆	Server Management	Bit9 Software Reputation Service proxy cleared	141	Info	Proxy disabled. Using direct connection to Bit9 Software Reputation Service. ***Change Notes:*** *In pre-7.2.0 releases, the subtype referred to "Parity Knowledge Service".*
☆	Server Management	Bit9 Software Reputation Service proxy set	140	Info	Using proxy '$param1$' for connection to Bit9 Software Reputation Service. ***Change Notes:*** *In pre-7.2.0 releases, the subtype referred to "Parity Knowledge 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. ***Change Notes:*** *In 7.2.2, the description was slightly modified.*
	Server Management	Database verification error	108	Error	Bit9 Server database is corrupt: $param1$.
★	Server Management	Enabled Indicator Set deleted	169	Info	Indicator Set $setName$ was deleted by '$username$' ***Note:*** *This event 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:*** *Not new but undocumented prior to v7.2.0. 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 '$provider$'. ***Change Notes:*** *New in 7.0.0 Patch 10 and 7.0.1 Patch 7.*

● New for v7.2.2 ○ Changed for v7.2.2 ♣ New for v7.2.1 ♧ Changed for v7.2.1 ★ New for v7.2.0 ☆ Changed for v7.2.0
♦ New for v7.0.1 ◊ Changed for v7.0.1 ▲ New for v7.0.0 Δ Changed for v7.0.0 X Deleted from v7.0.0

	Type	Subtype	ID No.	Severity	Example Descriptions/Comments
♦	Server Management	File analysis completed	161	Info Warning	File '$filename$' [$hash$] was successfully analyzed with '$provider$'. Nothing suspicious was found. or File '$filename$' [$hash$] was successfully analyzed with '$provider$'. It was reported as malicious. ***Change Notes:*** *New in 7.0.0 Patch 10 and 7.0.1 Patch 7.*
♦	Server Management	File analysis error	160	Error	Analysis of file '$filename$' [$hash$] with '$provider$' failed because of error '$param1$'. ***Change Notes:*** *New in 7.0.0 Patch 10 and 7.0.1 Patch 7.*
★	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 '$ruleName$'. ***Change Notes:*** *New in 7.0.0 Patch 10 and 7.0.1 Patch 7.*
♣	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$''
♣	Server Management	Health indicator changed	183	Info	The System has updated Health indicator $Param1$ on tab $Param2$ on the System Health page. ***Notes:*** *Param1 is the name of the health indicator. Param2 is the name of the tab on which the health indicator appears.*
○ ♣	**Server Management**	**Health indicator created**	182	Info	A new health indicator $Param1$ was created by $username$ on the tab '$Param2$' of the System Health page. *Notes:* *Param1 is the name of the health indicator.* *Param2 is the name of the tab on which the health indicator appears.* ***Change Notes:*** *In 7.2.2, the description was modified and the username parameter was added to it.*
♣	Server Management	Health indicator deleted	184	Info	The system has removed health indicator $Param1$ from tab $Param2$ on the System Health Page. ***Notes:*** *Param1 is the name of the health indicator. Param2 is the name of the tab on which the health indicator previously appeared.*
♣	Server Management	Health indicator severity change	181	Warning /Info	***For existing health indicators:*** 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.

● New for v7.2.2 ○ Changed for v7.2.2 ♣ New for v7.2.1 ♧ Changed for v7.2.1 ★ New for v7.2.0 ☆ Changed for v7.2.0
♦ New for v7.0.1 ◊ Changed for v7.0.1 ▲ New for v7.0.0 Δ Changed for v7.0.0 X Deleted from v7.0.0

	Type	Subtype	ID No.	Severity	Example Descriptions/Comments
★	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	License added	115	Notice	User '$username$' has successfully added new Bit9 Platform license.
	Server Management	License error	116	Error	User '$username$' attempted to add Bit9 Platform license. ($param1$)
★	Server Management	License warning	117	Warning	Your Bit9 Suite license will expire in $param1$ day(s) on $date$.
★	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	Reporter restart	151	Warning	Reporter started, build information: $param1
▲	Server Management	Reporter shutdown	152	Notice	Reporter shutdown cleanly.

● New for v7.2.2 ○ Changed for v7.2.2 ♣ New for v7.2.1 ♧ Changed for v7.2.1 ★ New for v7.2.0 ☆ Changed for v7.2.0
♦ New for v7.0.1 ◊ Changed for v7.0.1 ▲ New for v7.0.0 Δ Changed for v7.0.0 X Deleted from v7.0.0

	Type	Subtype	ID No.	Severity	Example Descriptions/Comments
	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.
	Server Management	Server config list error	113	Error	Data is bad for config list entry. Id[$param1$], Version[$param2$], Data[$param3$].
∆ ♧	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 '$username$' ***Change Notes:*** *Description was modified for 7.0.0. Triggering condition for disabling/enabling tracking of Microsoft support files was added for 7.2.1.*
∆	Server Management	Server error	142	Error/ Warning	There are too many descriptions to list for this subtype since it handles many different types of errors. Examples include: Bit9 Software Reputation Service - error logged and service resuming operation. The remote server returned an unexpected response: (413) Request Entity Too Large. ***Change Notes:*** *In 6.0.x, subtype was "Reporter error" and the only priority was "Error".*
★	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	Bit9 Server started, build information: $param1$.
	Server Management	Server shutdown	100	Warning	Bit9 Server shutdown cleanly.
☆	Server Management	Server upgrade failed	112	Error	Failed to upgrade Bit9 Server to $param1$. Contact support. ***Change Notes:*** *The event description referred to "Parity Server" in pre-v7.2.0 releases.*
☆	Server Management	Server upgrade succeeded	111	Info	Successfully upgraded Bit9 Server to version $param1$. ***Change Notes:*** *The event description referred to "Parity Server" in pre-v7.2.0 releases.*
◊	Server Management	SSL certificate CN mismatch	128	Critical	Common Name mismatch between SSL certificate ($param1$) and RPC Server Name ($param2$). ***Change Notes:*** *Subtype was "Common name mismatch" in previous versions.*
◊	Server Management	SSL certificate error	127	Critical	Server was not able to use default SSL certificate. Communication with agents is disabled. ***Change Notes:*** *Subtype was "Agent communication disabled" in pre-7.0.1 versions.*
◊	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. ***Change Notes:*** *Subtype was "Certificate expired" in pre-7.0.1 versions.*
◊	Server Management	SSL certificate expiring	124	Critical	Server SSL certificate will expire on $param1$. ***Change Notes:*** *Subtype was "Certificate expiring" in pre-7.0.1 versions.*
◊	Server Management	SSL certificate generated	118	Notice	User '$username$' has successfully generated a new SSL certificate for Bit9 Server: $param1$ ***Change Notes:*** *Subtype was "New certificate generated" in pre-7.0.1 versions.*

● New for v7.2.2 ○ Changed for v7.2.2 ♣ New for v7.2.1 ♧ Changed for v7.2.1 ★ New for v7.2.0 ☆ Changed for v7.2.0
♦ New for v7.0.1 ◊ Changed for v7.0.1 ▲ New for v7.0.0 ∆ Changed for v7.0.0 X Deleted from v7.0.0

	Type	Subtype	ID No.	Severity	Example Descriptions/Comments
◊	Server Management	SSL certificate generation failed	119	Warning	User '$username$' has failed to generate a new SSL certificate for Bit9 Server. Error: $param1$ ***Change Notes:*** *Subtype was "New certificate generation failed" in pre-7.0.1 versions.*
◊	Server Management	SSL certificate import failed	121	Warning	User '$username$' has failed to import new SSL certificate for Bit9 Server. Error: $param1$ ***Change Notes:*** *Subtype was "Certificate import failed" in previous versions.*
◊	Server Management	SSL certificate imported	120	Notice	User '$username$' has successfully imported a new SSL certificate for Bit9 Server: $param1$ ***Change Notes:*** *Subtype was "Certificate imported" in pre-7.0.1 versions.*
	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 Bit9 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	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 Bit9 Software Reputation Service
★	Server Management	Updaters Indicator Set enabled	170	Info	'$username$' enabled automatic update of Indicator Sets from Bit9 Software Reputation Service
★	Server Management	Updaters update disabled	150	Info	'$username$' disabled automatic update of Application Updaters from Bit9 Software Reputation Service
★	Server Management	Updaters update enabled	149	Info	'$username$' enabled automatic update of Application Updaters from Bit9 Software Reputation Service
	Session Management	Console user created	302	Info	'$username$' created new username $param1$.
	Session Management	Console user deleted	303	Info	'$username$' deleted the user '$param1$'.
	Session Management	Console user login	300	Info	User '$username$' logged in from $ipaddress$.
	Session Management	Console user logout	301	Info	User '$username$' logged out.
	Session Management	Console user modified	304	Info	'$username$' changed the access level for $consoleuser$ from '$usergroup1$' to '$usergroup2$'. '$username$' changed the password for '$consoleuser$'. **Note:** The access levels are the "Group" values on the Login Accounts pages.
	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 group created	306	Info	User group '$param1$' created by '$username$'
▲	Session Management	User group deleted	307	Info	User group '$param1$' deleted by '$username$'
▲	Session Management	User group modified	308	Info	User group '$param1$' modified by '$username$'

● New for v7.2.2 ○ Changed for v7.2.2 ♣ New for v7.2.1 ♧ Changed for v7.2.1 ★ New for v7.2.0 ☆ Changed for v7.2.0
♦ New for v7.0.1 ◊ Changed for v7.0.1 ▲ New for v7.0.0 Δ Changed for v7.0.0 X Deleted from v7.0.0

Section 2: Access to Bit9 Event Data

In addition to the Bit9 Console user interface, event data is available in the following ways:

- as Syslog output, in one of four formats
- as Bit9 "external event logging" output
- as SQL views through the Bit9 "Live Inventory SDK"
- as JSON output to external analytics services
- in event archive files

Syslog Formats

The Bit9 Security Platform supports integration of its event information with Syslog servers using several formats. You configure Syslog integration on the System Configuration/Events page, described in the "Bit9 Configuration" chapter of the *Using the Bit9 Security Platform* guide or online Help in the Bit9 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 Bit9 event logs with HP ArcSight ESM or HP ArcSight Logger
- **LEEF (IBM Q1 Labs)** – the format to user to integrate Bit9 event logs with IBM Security QRadar Log Manager or IBM Security QRadar SIEM

Note
If you worked with Bit9 Technical Support to manually enable special Syslog formatting in pre-6.0.2 releases, your changes will be overwritten on upgrade to this version of the Bit9 Security Platform. See "Setting Up External Event Logging" in the *Using the Bit9 Security Platform* guide for instructions on configuring the Bit9 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, ProcID, and MsgID. Table 4 shows the fields for the Basic and Enhanced Syslog formats supported by Bit9. Examples of messages in these formats are shown below the table.

Table 4. Bit9 Event Mapping to Basic and Enhanced Syslog Formats

Syslog field	Data Type	Note
Facility[1]	INTEGER	Syslog facility, always "user-level"
Severity[1]	INTEGER	Severity mapped from event priority (see Table 2)
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)	Bit9 Server hostname, appended by domain as per RFC 5424
App-Name	NVARCHAR(256)	(Enhanced Syslog only) Configurable value in ParityReporter.log.xml, by default "-"

Syslog field		Data Type	Note
ProcID		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 "*Bit9 Server event:*" and including all the "All messages" fields below inline; the message also can include some combination of the conditional fields. ***Bit9 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 Bit9 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 Bit9 policy for the agent associated with the event (Conditional)
	ban_name	NVARCHAR(128)	For files blocked due to bans, name of the ban (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) ***Change Notes:*** New for v7.2.0.
	server_version	NVARCHAR(MAX)	Version of the Bit9 Server associated with the event (All messages)
	file_trust	-2 pending -1 unknown 0-10 Trust value	File trust from the Bit9 SRS of the file associated with the event. Pending implies that SRS lookup was not yet performed but will be. (Conditional)
	file_threat	-2 pending -1 unknown 0 No threat 1 Potential risk 2 Malicious	File threat from the Bit9 SRS of the file associated with the event. Pending implies that SRS lookup was not yet performed but will be. (Conditional)

Syslog field		Data Type	Note
	Message fields (continued)		
	process_key	UID	Unique proprietary key identifying the instance of the process on a specific computer ***Change Notes:*** New for v7.2.0.
	process_trust	-2 pending -1 unknown 0-10 Trust value	Parent process trust from the Bit9 SRS of the file associated with the event. Pending implies that SRS lookup was not yet performed but will be. (Conditional) ***Change Notes:*** New for v7.2.0.
	process_threat	-2 pending -1 unknown 0 No threat 1 Potential risk 2 Malicious	Parent process threat from the Bit9 SRS of the file associated with the event. Pending implies that SRS lookup was not yet performed but will be. (Conditional) ***Change Notes:*** New for v7.2.0.
[1] Facility and Severity are coded into one number as per Syslog specification.			

Basic Syslog Format Message

The following is an example of Basic Syslog format:

```
16/06/14 13:42:48
Info message from: 123.45.67.8
Hostname: desktop8
Bit9 Server event: text="File 'c:\apps\alexainstaller.exe'
[07693beb9aaebdd8b3223a5becc25b44c70afd73cec9e4984ffc4e89624c5e17] was
executed for the first time." type="Discovery" subtype="First execution on
network" hostname="WORKGROUP\AVANTIME" username="AVANTIME\Administrator"
date="6/16/2014 1:42:48 PM" ip_address="fe80::e82f:d94b:f54f:bd50"
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="7.2.2.899" 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:

```
16/06/14 14:38:37
Notice message from 123.45.67.8
Hostname: desktop8
1 2014-06-16T14:38:37Z avantime - - - - Bit9 Server event:  text="Computer
WORKGROUP\AVANTIME discovered new file 'c:\windows\temp\jvyyqbe4.dll'
[eeb0ada676b1f8e5e94015b5e48ed4bcf23959b0d0837bbd51c1870f5d641d2a]."
type="Discovery" subtype="New unapproved file to computer"
hostname="WORKGROUP\AVANTIME" username="NT AUTHORITY\SYSTEM" date="6/16/2014
2:38:35 PM" ip_address="fe80::e82f:d94b:f54f:bd50"
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="7.2.2.992" file_trust="-1" file_threat="-1"
```

Mapping Bit9 Events to ArcSight CEF

The Bit9 Security Platform 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 Bit9 event logs with ArcSight ESM or ArcSight Logger. You configure Syslog integration on the System Configuration/Events page, described in the "Bit9 Configuration" chapter of *Using the Bit9 Security Platform*.

This section describes the mapping of Bit9 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. Bit9 Event Mapping to Syslog ArcSight Common Event Format (RFC 3164 and ArcSight CEF)

Syslog field	Data Type	Note
Facility[1]	INTEGER	Syslog facility; always "user-level"
Severity[1]	INTEGER	Severity mapped from event priority (see Table 2)
Timestamp	DATETIME	Timestamp when the Syslog event was sent (without the year, according to RFC 3164)
Hostname	NVARCHAR(256)	Bit9 Server hostname
Message		Message encoded according to ArcSight CEF specification

[1] Facility and Severity are coded into one number as per Syslog specification.

Message Format

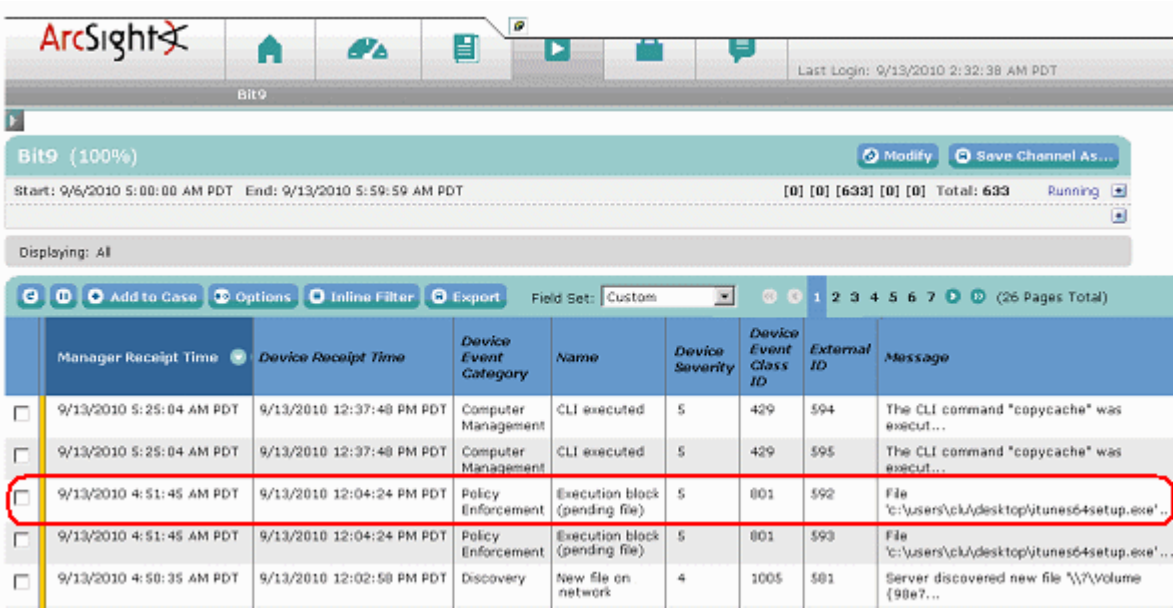
ArcSight CEF format uses the Syslog message protocol as a transport mechanism. The format of the message is as follows:

```
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 Bit9:

```
Sep 19 08:26:10 server3 CEF:0|Bit9|Security
Platform|7.2.2.899|801|Execution block (unapproved file)|5| dst=10.0.0.1
duser=NTAUTHORITY\SYSTEM msg=File 'itunessetup64.exe' has been blocked for
execution.
```



CEF-Bit9 Mapping Tables

The tables below provide the following CEF-Bit9 mapping information:

- Table 6 shows the mapping of Bit9 data to CEF Header fields
- Table 7 shows the mapping of Bit9 data to CEF Extension field data
- Table 8 shows Bit9-specific custom extensions

Table 6. Mapping of Bit9 Event Data to CEF Header Fields

CEF Prefix Field	Bit9 Value	Description
Host	Hostname	Hostname of the Bit9 Server from which Syslog output is provided
Version	0	CEF format version. By default this is 0.
Device Vendor	Bit9	The company name of the syslog output provider.
Device Version	7.2.2.*xxx*	The version of product generating syslog output. The current Bit9 version is 7.2.2 and *xxx* represents the three-digit build number appended to the version.
Device Product	Security Platform	The product name of the syslog output provider.
SignatureID	Event subtype ID	Unique number identifying the event subtype as classified by Bit9.
Name	Event subtype name	Unique name identifying the event subtype as classified by Bit9.
Severity	Event severity ID	Numeric value indicating the severity of the event. Bit9 event severity ranges from 7 (least severe) to 0 (most severe). These values are mapped to CEF severity levels, which range from 0 (least severe) to 10 (most severe). The CEF severity is calculated by subtracting the Bit9 severity from 9. This means that the most severe Bit9 event has a CEF severity of 9. The least severe Bit9 event has a CEF severity of 2.
Extension	*(varies)*	Additional event information. See the Extension Fields mapping table.

Table 7. Mapping of Bit9 Event Data to CEF Extensions

CEF Extension Name	Bit9 Event Field	Description
externalId	Event ID	Unique auto-incremented ID of each generated Bit9 event.
deviceEventCategory	Event Type	Bit9 event type
startTime Δ	Event Timestamp	Timestamp when the event was created on the endpoint (in UTC).
ReceiptTime Δ	Event Received Timestamp	Timestamp when the event was received by the Bit9 Server (in UTC).
message	Event Description	Full text message of the Bit9 event
deviceHostName	Server Hostname	Bit9 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 * Δ	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	File hash of the file generating the event (SHA-256).
deviceProcessName *	Process	Process name of the process generating the event.
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)

* CEF Extensions with asterisks are context-dependent and not available on all events.

Δ CEF Extensions shown with the delta symbol were new or changed mappings for Parity 7.0.0.

☆ CEF Extensions shown with the star were new or changed mappings for Parity 7.2.0.

Table 8. Mapping to Custom CEF Extensions

CEF Custom Extension & Label	Bit9 Event Field	Description
deviceCustomString1 * deviceCustomString1Label = "rootHash"	Root Hash	Root hash of the file generating the event. Context-dependent and not available on all events.
deviceCustomString2 * deviceCustomString2Label = "installerFilename"	Installer Filename	Installer Filename of the file generating the event. Context-dependent and not available on all events.
deviceCustomString3 * deviceCustomString3Label = "policy"	Policy	Bit9 Policy of the machine generating the event. Context-dependent and not available on all events.
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)
deviceCustomFloatingPoint1 * deviceCustomFloatingPoint1Label = "fileTrust"	File Trust	File trust from the Bit9 SRS of the file associated with the event. Pending implies that SRS 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 the Bit9 SRS of the file associated with the event. Pending implies that SRS 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 the Bit9 SRS of the file associated with the event. Pending implies that SRS lookup was not yet performed but will be. (Conditional) -2 pending -1 unknown 0-10 Trust value

CEF Custom Extension & Label	Bit9 Event Field	Description
deviceCustomFlexString2* ☆ deviceCustomFlexString2Label = “processThreat”	Process Threat	Parent process threat from the Bit9 SRS of the file associated with the event. Pending implies that SRS 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.
Δ CEF Extensions shown with the delta symbol were new or changed mappings for Parity 7.0.0.
◊ CEF Extensions shown with the diamond symbol were new or changed mappings for Parity 7.0.1 Patch 3.
☆ CEF Extensions shown with the star were new or changed mappings for Parity 7.2.0 Patch 5.

Mapping Bit9 Events to Q1Labs LEEF Format

The Bit9 Security Platform supports integration of its event information with Syslog servers using several formats. One of the Syslog formats supported is Q1Labs LEEF (Log Event Extended Format), which you can use to integrate Bit9 event logs with QRadar SIEM or QRadar Log Manager.

You configure Syslog integration in the Bit9 Console, on the Events section of the System Configuration page.

This section describes setup of QRadar Log Manager to accept Bit9 events, and the mapping of Bit9 event fields to Q1Labs LEEF fields. See your QRadar documentation for full information about QRadar and LEEF capabilities.

Important: If you are running **Bit9 Server 7.2.1 P7 or later**, you must update the QRadar DSM for Bit9 to at least the June 2015 version. Otherwise, all Bit9 events will appear as 'unknown' in LEEF.

Configuring QRadar Log Manager

When a Bit9 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 Bit9, and will add a Log source definition for that Bit9 Server called "Bit9Parity @ *Bit9ServerComputerName*" with the default QRadar Log Manager parameters.

To be certain you capture all events, set up Bit9 as a log source in QRadar Log Manager *before* integrating with the Bit9 Server.

Manual Setup of Bit9 as Event Source

You can manually configure Bit9 as the source of events sent to the QRadar Log Manager.

To configure Bit9 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 **Bit9 Parity**.
5. For Log Source Description, enter **Bit9 Parity Server**.
6. Choose **Bit9 Parity** on the Log Source menu.
7. For Log Source Identifier, enter the fully qualified domain name of the Bit9 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. Bit9 Event Mapping to Q1Labs Log Event Enhanced Format (RFC 3164 and Q1Labs LEEF)

Syslog field	Data Type	Note
Facility[1]	INTEGER	Syslog facility; always "user-level"
Severity[1]	INTEGER	Severity mapped from Bit9 event severity (see Table 2)
Timestamp	DATETIME	Timestamp when the Syslog event was sent (without the year, according to RFC 3164)
Hostname	NVARCHAR(256)	Bit9 Server hostname
Message		Message encoded according to Q1Labs LEEF specification
[1] Facility and Severity are coded into one number as per Syslog specification.		

LEEF Format

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

```
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 Bit9, with "*<tab>*"substituted where actual tabs are used in the message:

```
Jan 18 11:07:53 192.168.1.1 LEEF:1.0|QRadar|QRM|1.0<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
```

LEEF-Bit9 Mapping Tables

The tables below provide the following LEEF-Bit9 mapping information:

- Table 10 shows the mapping of Bit9 event data to LEEF Header fields
- Table 11 shows the mapping of Bit9 events to LEEF Attributes

Table 10. Mapping of Bit9 Event Data to LEEF Header Fields

LEEF Prefix Field	Bit9 Value	Description
Hostname	Hostname	Hostname of the Bit9 Server from which Syslog output is provided
LEEF Version	1.0	LEEF format version. By default this is 1.0.
Vendor	Bit9	The company name of the Syslog output provider.
Product*	Security Platform	The name of the product generating Syslog output. * ***Change Notes:*** Prior to v7.2.1 Patch 7, the value of this field was "Parity".

LEEF Prefix Field	Bit9 Value	Description
Version	7.2.1.xxx	The version of the product generating Syslog output, including the three-digit build number (represented here by "xxx"). The current Bit9 Security Platform version is 7.2.2.
EventID	Event subtype name	Unique name identifying the event subtype as classified by Bit9.
Attributes	(varies)	See the LEEF Attributes mapping table.

Table 11. Mapping of Bit9 Event Fields to LEEF Attributes

LEEF Attribute (name in RAW view)	LEEF Property (Visible name in Console)	Regular Expression (to Extract)	Bit9 Event Field	Description
cat	Category		Event Type	Bit9 event category name
sev	Severity		Severity	Severity of the Bit9 event. Mapped from Bit9 range 7-0 (0 is most important) into LEEF range 1-10 (10 is the most important)
devTime	Device Time		Event Timestamp	Timestamp (UTC) when Bit9 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 Bit9 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

LEEF Attribute (name in RAW view)	LEEF Property (Visible name in Console)	Regular Expression (to Extract)	Bit9 Event Field	Description
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
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	Bit9 Policy of the computer generating the event
dstHostName[1]	Destination Hostname	dstHostName=([^\t]+)[\t]*	Hostname	Hostname of the Bit9 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 the Bit9 SRS of the file associated with the event. Pending implies that SRS 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)	Bit9 Event Field	Description
fileThreat	File Threat	fileThreat=([^\t]+)[\t]*	File Threat	File threat from the Bit9 SRS of the file associated with the event. Pending implies that SRS 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 the Bit9 SRS of the file associated with the event. Pending implies that SRS 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 the Bit9 SRS of the file associated with the event. Pending implies that SRS lookup was not yet performed but will be. (Conditional) -2 pending -1 unknown 0 No threat 1 Potential risk 2 Malicious

[1] These are custom LEEF attributes for Bit9 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 Bit9 Custom Properties for instructions.

[2] These LEEF Extensions are context-dependent and not available on all events.

▲ LEEF Extensions with the delta symbol were new mappings beginning with Parity 7.0.0 Patch 6.

◊ LEEF Extensions with the diamond symbol were new or changed beginning with Parity 7.0.1 Patch 3.

☆ LEEF Extensions shown in bold with the star were new or changed mappings for Parity 7.2.0.

Manual Setup of Bit9 Custom Properties

For the current release of QRadar Log Manager, manual setup is required to parse certain Bit9 properties. Table 11 shows the regular expressions that must be used to parse each custom property.

To configure Bit9 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 **Bit9 Parity** 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 Bit9 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

The Bit9 Server allows users to send events to an external database. The following table describes the external events table columns.

Table 12. Bit9 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 Δ	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 Δ	VARCHAR(40)	IP address associated with the event ***Change Notes:*** *Data Type changed for 7.0.0.*
platform Δ	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

External table column	Data Type	Note
file_trust	INTEGER	File trust from the Bit9 SRS of the file associated with the event. Pending implies that SRS lookup was not yet performed but will be. (Conditional) **-2 pending** **-1 unknown** **0-10 Trust value**
file_threat	INTEGER	File threat from the Bit9 SRS of the file associated with the event. Pending implies that SRS 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 the Bit9 SRS of the file associated with the event. Pending implies that SRS lookup was not yet performed but will be. (Conditional) **-2 pending** **-1 unknown** **0-10 Trust value**
process_threat	INTEGER	Parent process threat from the Bit9 SRS of the file associated with the event. Pending implies that SRS lookup was not yet performed but will be. (Conditional) **-2 pending** **-1 unknown** **0 No threat** **1 Potential risk** **2 Malicious**
☆ New or changed for Bit9 Platform 7.2.0. ♦ New for Parity v7.0.1 Patch 3. Δ New or changed for Parity v7.0.0.		

Live Inventory SDK

Bit9 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 *Using the Bit9 Security Platform* guide or online Help in the Bit9 Console for more details.

Event Output for External Analytics

A Bit9 Server can be configured to send data, including Bit9 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 Bit9 Data for External Analysis" in the *Using the Bit9 Security Platform* guide or online Help in the Bit9 Console for more details.

Archive Files

By default, the Bit9 Server exports a daily archive of events to a GZIP-compressed CSV file named in the format *yyyy-mm-dd.***csv**.**gz**. 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')
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) ***Change Notes:*** *New for v7.2.0.*
FILE_TRUST	File trust from the Bit9 SRS of the file associated with the event. Pending implies that SRS lookup was not yet performed but will be. (Conditional) **-2 pending** **-1 unknown** **0-10 Trust value**

Archive CSV column	Note
FILE_THREAT	File threat from the Bit9 SRS of the file associated with the event. Pending implies that SRS 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 the Bit9 SRS of the file associated with the event. Pending implies that SRS lookup was not yet performed but will be. (Conditional) **-2 pending** **-1 unknown** **0-10 Trust value**
PROCESS_THREAT	Parent process threat from the Bit9 SRS of the file associated with the event. Pending implies that SRS 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