Understanding Intrusion and Correlation Data Structures

The eStreamer service transmits a number of data record types to deliver requested events and metadata to the client. This chapter describes the structures of data records for the following types of event data:

- intrusion events data and event extra data generated by managed devices
- correlation (compliance) events generated by the Defense Center
- metadata records

The following section in this chapter define the event message structures:

- Intrusion Event and Metadata Record Types, page 3-1.

For a general overview of eStreamer's message format for transmitting data records, see Event Data Message Format, page 2-17.

Intrusion Event and Metadata Record Types

The table that follows lists all currently supported record types for intrusion events, intrusion event extra data, and metadata messages. The data for these record types is in fixed-length fields. By contrast, correlation event records contain one or more levels of nested data blocks with variable lengths. The table below provides a link to the chapter subsection that defines the associated data record structure.

For some record types, eStreamer supports more than one version. The table indicates the status of each version (current or legacy). A current record is the latest version. A legacy record has been superseded by a later version but can still be requested from eStreamer.

Table 3-1 Intrusion Event and General Metadata Record Types

Record Type	Block Type	Series	Description	Record Status	Data Format Described in...
2	N/A	N/A	Packet Data (Version 4.8.0.2+)	Current	Packet Record 4.8.0.2+, page 3-4
4	N/A	N/A	Priority Metadata	Current	Priority Record, page 3-5
9	20	1	Intrusion Impact Alert	Legacy	Intrusion Impact Alert Data, page B-29
9	153	1	Intrusion Impact Alert	Current	Intrusion Impact Alert Data 5.3+, page 3-12
62	N/A	N/A	User Metadata	Current	User Record, page 3-15

Table 3-1 Intrusion Event and General Metadata Record Types (continued)

Record Type	Block Type	Series	Description	Record Status	Data Format Described in...
66	N/A	N/A	Rule Message Metadata (Version 4.6.1+)	Current	Rule Message Record for 4.6.1+, page 3-16
67	N/A	N/A	Classification Metadata (Version 4.6.1+)	Current	Classification Record for 4.6.1+, page 3-17
69	N/A	N/A	Correlation Policy Metadata (Version 4.6.1+)	Current	Correlation Policy Record, page 3-18
70	N/A	N/A	Correlation Rule Metadata (Version 4.6.1+)	Current	Correlation Rule Record, page 3-20
104	N/A	N/A	Intrusion Event (IPv4) Record 4.9 - 4.10.x	Legacy	earlier versions of the product
105	N/A	N/A	Intrusion Event (IPv6) Record 4.9-4.10.x	Legacy	earlier versions of the product
110	4	2	Intrusion Event Extra Data (Version 4.10.0+)	Current	Intrusion Event Extra Data Record, page 3-21
111	5	2	Intrusion Event Extra Data Metadata (Version 4.10.0+)	Current	Intrusion Event Extra Data Metadata, page 3-23
112	128	1	Correlation Event for 5.1+	Current	Correlation Event for 5.1+, page 3-36
115	14	2	Security Zone Name Metadata	Current	Security Zone Name Record, page 3-25
116	14	2	Interface Name Metadata	Current	Interface Name Record, page 3-26
117	14	2	Access Control Policy Name Metadata	Current	Access Control Policy Name Record, page 3-27
118	15	2	Intrusion Policy Name Metadata	Current	Intrusion Policy Name Record, page 4-20
119	15	2	Access Control Rule ID Metadata	Current	Access Control Rule ID Record Metadata, page 3-28
120	N/A	N/A	Access Control Rule Action Metadata	Current	Access Control Rule Action Record Metadata, page 4-21
121	N/A	N/A	URL Category Metadata	Current	URL Category Record Metadata, page 4-22
122	N/A	N/A	URL Reputation Metadata	Current	URL Reputation Record Metadata, page 4-23
123	N/A	N/A	Managed Device Metadata	Current	Managed Device Record Metadata, page 3-30
125	N/A	2	Malware Event Record (Version 5.1.1+)	Current	Malware Event Record 5.1.1+, page 3-30
125	24	2	Malware Event (Version 5.1.1+)	Current	Malware Event Data Block 5.1.1.x, page B-36
125	33	2	Malware Event (Version 5.2.x)	Legacy	Malware Event Data Block 5.2.x, page B-42
125	35	2	Malware Event (Version 5.3)	Legacy	Malware Event Data Block 5.3, page B-48
125	44	2	Malware Event (Version 5.3.1+)	Current	Malware Event Data Block 5.3.1+, page 3-64

Table 3-1 Intrusion Event and General Metadata Record Types (continued)

Record Type	Block Type	Series	Description	Record Status	Data Format Described in...
127	14	2	Collective Security Intelligence Cloud Name Metadata (Version 5.1+)	Current	Collective Security Intelligence Cloud Name Metadata, page 3-31
128	N/A	N/A	Malware Event Type Metadata (Version 5.1+)	Current	Malware Event Type Metadata, page 3-33
129	N/A	N/A	Malware Event Subtype Metadata (Version 5.1+)	Current	Malware Event Subtype Metadata, page 3-34
130	N/A	N/A	FireAMP Detector Type Metadata (Version 5.1+)	Current	FireAMP Detector Type Metadata, page 3-34
131	N/A	N/A	FireAMP File Type Metadata (Version 5.1+)	Current	FireAMP File Type Metadata, page 3-35
160	150	1	IOC State Data Block for 5.3+	Current	IOC State Data Block for 5.3+, page 4-25
161	39	2	IOC Name Data Block for 5.3+	Current	IOC Name Data Block for 5.3+, page 4-27
207	N/A	N/A	Intrusion Event (IPv4) Record 5.0.x - 5.1	Legacy	Intrusion Event (IPv4) Record 5.0.x - 5.1, page B-2
208	N/A	N/A	Intrusion Event (IPv6) Record 5.0.x - 5.1	Legacy	Intrusion Event (IPv6) Record 5.0.x - 5.1, page B-6
260	19	2	ICMP Type Data Data Block	Current	ICMP Type Data Block, page 3-53
270	20	2	ICMP Code Data Block	Current	ICMP Code Data Block, page 3-54
400	34	2	Intrusion Event Record 5.2.x	Legacy	Intrusion Event Record 5.2.x, page B-11
400	41	2	Intrusion Event Record 5.3	Legacy	Intrusion Event Record 5.3, page B-17
400	42	2	Intrusion Event Record 5.3.1+	Current	Intrusion Event Record 5.3.1+, page 3-6
500	32	2	File Event (Version 5.2.x)	Legacy	File Event for 5.2.x, page B-112
500	38	2	File Event (Version 5.3)	Legacy	File Event for 5.3, page B-116
500	43	2	File Event (Version 5.3.1+)	Current	File Event for 5.3.1+, page 3-57
502	32	2	File Event (Version 5.2.x)	Legacy	File Event for 5.2.x, page B-112
502	38	2	File Event (Version 5.3)	Legacy	File Event for 5.3, page B-116
502	43	2	File Event (Version 5.3.1+)	Current	File Event for 5.3.1+, page 3-57
N/A	27	2	File Event SHA Hash for 5.3+	Current	File Event SHA Hash for 5.3+, page 3-71
511	27	2	Rule Documentation Data Block for 5.2+	Current	Rule Documentation Data Block for 5.2+, page 3-73
520	28	2	Geolocation Data Block for 5.2+	Current	Geolocation Data Block for 5.2+, page 3-76

Packet Record 4.8.0.2+

The eStreamer service transmits the packet data associated with an event in a Packet record, the format of which is shown below. Packet data is sent when the Packet flag—bit 0 in the Request Flags field of a request message—is set. See Request Flags, page 2-11. If you enable bit 23, an extended event header is included in the record. Note that the Record Type field, which appears after the Message Length field, has a value of 2, indicating a packet record.

Byte	0								1								2								3							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Header Version (1)																	Message Type (4)															
Message Length																																
Record Type (2)																																
Record Length																																
eStreamer Server Timestamp (in events, only if bit 23 is set)																																
Reserved for Future Use (in events, only if bit 23 is set)																																
Device ID																																
Event ID																																
Event Second																																
Packet Second																																
Packet Microsecond																																
Link Type																																
Packet Length																																
Packet Data...																																

The following table describes the fields in the Packet record.

Table 3-2 Packet Record Fields

Field	Data Type	Description
Device ID	uint32	The device identification number. You can obtain device names that correlate to them by requesting Version 3 or 4 metadata. See Managed Device Record Metadata, page 3-30 for more information.
Event ID	uint32	The event identification number.
Event Second	uint32	The second (from 01/01/1970) that the event occurred.
Packet Second	uint32	The second (from 01/01/1970) that the packet was captured.

Table 3-2 Packet Record Fields (continued)

Field	Data Type	Description
Packet Microsecond	uint32	Microsecond (one millionth of a second) increment that the packet was captured.
Link Type	uint32	Link layer type. Currently, the value will always be `1` (signifying the Ethernet layer).
Packet Length	uint32	Number of bytes included in the packet data.
Packet Data	variable	Actual captured packet data (header and payload).

Priority Record

The eStreamer service transmits the priority associated with an event in a Priority record, the format of which is shown below. (Priority information is sent when one of the metadata flags—bits 1, 14, 15, or 20 in the Request Flags field of a request message—is set. See Request Flags, page 2-11.) Note that the Record Type field, which appears after the Message Length field, has a value of `4`, indicating a Priority record.

Byte	0								1								2								3							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Header Version (1)																	Message Type (4)															
Message Length																																
Record Type (4)																																
Record Length																																
Priority ID																																
Name Length																	Priority Name...															

The following table describes each priority-specific field.

Table 3-3 Priority Record Fields

Field	Data Type	Description
Priority ID	uint32	Indicates the priority identification number.
Name Length	uint16	Number of bytes included in the priority name.
Priority Name	variable	Priority name that corresponds with the priority ID (1 - high, 2 - medium, 3 - low).

Intrusion Event Record 5.3.1+

The fields in the intrusion event record are shaded in the following graphic. The record type is 400 and the block type is 42 in the series 2 set of data blocks.

You can request 5.3.1+ intrusion events from eStreamer only by extended request, for which you request event type code 12 and version code 7 in the Stream Request message (see Submitting Extended Requests, page 2-4 for information about submitting extended requests).

For version 5.3.1+ intrusion events, the event ID, the managed device ID, and the event second form a unique identifier. The connection second, connection instance, and connection counter together form a unique identifier for the connection event associated with the intrusion event.

Byte	0								1								2								3							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Header Version (1)																	Message Type (4)															
Message Length																																
Record Type (400)																																
Record Length																																
eStreamer Server Timestamp (in events, only if bit 23 is set)																																
Reserved for Future Use (in events, only if bit 23 is set)																																
Block Type (42)																																
Block Length																																
Device ID																																
Event ID																																
Event Second																																
Event Microsecond																																
Rule ID (Signature ID)																																
Generator ID																																
Rule Revision																																
Classification ID																																
Priority ID																																

Byte	0								1								2								3							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Source IP Address Source IP Address, continued Source IP Address, continued Source IP Address, continued																																
Destination IP Address Destination IP Address, continued Destination IP Address, continued Destination IP Address, continued																																
Source Port or ICMP Type																	Destination Port or ICMP Code															
IP Protocol ID									Impact Flags								Impact								Blocked							
MPLS Label																																
VLAN ID																	Pad															
Policy UUID Policy UUID, continued Policy UUID, continued Policy UUID, continued																																
User ID																																
Web Application ID																																
Client Application ID																																
Application Protocol ID																																
Access Control Rule ID																																
Access Control Policy UUID Access Control Policy UUID, continued Access Control Policy UUID, continued Access Control Policy UUID, continued																																
Interface Ingress UUID																																

The following table describes each intrusion event record data field.

Table 3-4 Intrusion Event Record 5.3.1+ Fields

Field	Data Type	Description
Block Type	unint32	Initiates an Intrusion Event data block. This value is always `42`.
Block Length	unint32	Total number of bytes in the Intrusion Event data block, including eight bytes for the Intrusion Event block type and length fields, plus the number of bytes of data that follows.
Device ID	unit32	Contains the identification number of the detecting managed device. You can obtain the managed device name by requesting Version 3 or 4 metadata. See Managed Device Record Metadata, page 3-30 for more information.
Event ID	uint32	Event identification number.
Event Second	uint32	UNIX timestamp (seconds since 01/01/1970) of the event's detection.
Event Microsecond	uint32	Microsecond (one millionth of a second) increment of the timestamp of the event's detection.
Rule ID (Signature ID)	uint32	Rule identification number that corresponds with the event.
Generator ID	uint32	Identification number of the FireSIGHT System preprocessor that generated the event.
Rule Revision	uint32	Rule revision number.
Classification ID	uint32	Identification number of the event classification message.
Priority ID	uint32	Identification number of the priority associated with the event.
Source IP Address	uint8[16]	Source IPv4 or IPv6 address used in the event.
Destination IP Address	uint8[16]	Destination IPv4 or IPv6 address used in the event.
Source Port or ICMP Type	uint16	The source port number if the event protocol type is TCP or UDP, or the ICMP type if the event is caused by ICMP traffic.
Destination Port or ICMP Code	uint16	The destination port number if the event protocol type is TCP or UDP, or the ICMP code if the event is caused by ICMP traffic.
IP Protocol Number	uint8	IANA-specified protocol number. For example: • `0` - IP • `1` - ICMP • `6` - TCP • `17` - UDP

Table 3-4 Intrusion Event Record 5.3.1+ Fields (continued)

Field	Data Type	Description
Impact Flags	bits[8]	Impact flag value of the event. The low-order eight bits indicate the impact level. Values are: • `0x01` (bit 0) - Source or destination host is in a network monitored by the system. • `0x02` (bit 1) - Source or destination host exists in the network map. • `0x04` (bit 2) - Source or destination host is running a server on the port in the event (if TCP or UDP) or uses the IP protocol. • `0x08` (bit 3) - There is a vulnerability mapped to the operating system of the source or destination host in the event. • `0x10` (bit 4) - There is a vulnerability mapped to the server detected in the event. • `0x20` (bit 5) - The event caused the managed device to drop the session (used only when the device is running in inline, switched, or routed deployment). Corresponds to blocked status in the FireSIGHT System web interface. • `0x40` (bit 6) - The rule that generated this event contains rule metadata setting the impact flag to red. The source or destination host is potentially compromised by a virus, trojan, or other piece of malicious software. • `0x80` (bit 7) - There is a vulnerability mapped to the client detected in the event. (version 5.0+ only) The following impact level values map to specific priorities on the Defense Center. An `x` indicates the value can be `0` or `1`: • gray (0, unknown): `00X00000` • red (1, vulnerable): `XXXX1XXX, XXX1XXXX, X1XXXXXX, 1XXXXXXX` (version 5.0+ only) • orange (2, potentially vulnerable): `00X0011X` • yellow (3, currently not vulnerable): `00X0001X` • blue (4, unknown target): `00X00001`
Impact	uint8	Impact flag value of the event. Values are: • `1` - Red (vulnerable) • `2` - Orange (potentially vulnerable) • `3` - Yellow (currently not vulnerable) • `4` - Blue (unknown target) • `5` - Gray (unknown impact)
Blocked	uint8	Value indicating whether the event was blocked: • `0` - not blocked • `1` - blocked • `2` - would be blocked (but not permitted by configuration)

Table 3-4 Intrusion Event Record 5.3.1+ Fields (continued)

Field	Data Type	Description
MPLS Label	uint32	MPLS label.
VLAN ID	uint16	Indicates the ID of the VLAN where the packet originated.
Pad	uint16	Reserved for future use.
Policy UUID	uint8[16]	A policy ID number that acts as a unique identifier for the intrusion policy.
User ID	uint32	The internal identification number for the user, if applicable.
Web Application ID	uint32	The internal identification number for the web application, if applicable.
Client Application ID	uint32	The internal identification number for the client application, if applicable.
Application Protocol ID	uint32	The internal identification number for the application protocol, if applicable.
Access Control Rule ID	uint32	A rule ID number that acts as a unique identifier for the access control rule.
Access Control Policy UUID	uint8[16]	A policy ID number that acts as a unique identifier for the access control policy.
Ingress Interface UUID	uint8[16]	An interface ID number that acts as a unique identifier for the ingress interface.
Egress Interface UUID	uint8[16]	An interface ID number that acts as a unique identifier for the egress interface.
Ingress Security Zone UUID	uint8[16]	A zone ID number that acts as a unique identifier for the ingress security zone.
Egress Security Zone UUID	uint8[16]	A zone ID number that acts as a unique identifier for the egress security zone.
Connection Timestamp	uint32	UNIX timestamp (seconds since 01/01/1970) of the connection event associated with the intrusion event.
Connection Instance ID	uint16	Numerical ID of the Snort instance on the managed device that generated the connection event.
Connection Counter	uint16	Value used to distinguish between connection events that happen during the same second.
Source Country	uint16	Code for the country of the source host.
Destination Country	uint16	Code for the country of the destination host.
IOC Number	uint16	ID number of the compromise associated with this event.
Security Context	uint8(16)	ID number for the security context (virtual firewall) that the traffic passed through. Note that the system only populates this field for ASA FirePOWER devices in multi-context mode.

Intrusion Impact Alert Data 5.3+

The Intrusion Impact Alert 5.3+ event contains information about impact events. It is transmitted when an intrusion event is compared to the system network map data and the impact is determined. It uses the standard record header with a record type of 9, followed by an Intrusion Impact Alert data block with a series 1 data block type of 153 in the series 1 group of blocks. (The Impact Alert data block is a type of series 1 data block. For more information about series 1 data blocks, see Understanding Discovery (Series 1) Blocks, page 4-55.)

You can request that eStreamer only transmit intrusion impact events by setting bit 5 in the Flags field of the request message. See Event Stream Request Message Format, page 2-10 for more information about request messages. Version 1 of these alerts only handles IPv4. Version 2, introduced in 5.3, handles IPv6 events in addition to IPv4.

Byte	0								1								2								3							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Header Version (1)																	Message Type (4)															
Message Length																																
Record Type (9)																																
eStreamer Server Timestamp (in events, only if bit 23 is set)																																
Reserved for Future Use (in events, only if bit 23 is set)																																
Intrusion Impact Alert Block Length																																
Event ID																																
Device ID																																
Event Second																																
Impact																																
Source IP Address Source IP Address, continued Source IP Address, continued Source IP Address, continued																																
Destination IP Address Destination IP Address, continued Destination IP Address, continued Destination IP Address, continued																																

Byte	0								1								2								3							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Impact Description	String Block Type (0)																															
	String Block Length																															
	Description...																															

The following table describes each data field in an impact event.

Table 3-5 Impact Event Data Fields

Field	Data Type	Description
Intrusion Impact Alert Block Type	uint32	Indicates that an intrusion impact alert data block follows. This field will always have a value of `20`. See Intrusion Event and Metadata Record Types, page 3-1.
Intrusion Impact Alert Block Length	uint32	Indicates the length of the intrusion impact alert data block, including all data that follows and 8 bytes for the intrusion impact alert block type and length.
Event ID	uint32	Indicates the event identification number.
Device ID	uint32	Indicates the managed device identification number.
Event Second	uint32	Indicates the second (from 01/01/1970) that the event was detected.

Table 3-5 Impact Event Data Fields (continued)

Field	Data Type	Description
Impact	bits[8]	Impact flag value of the event. The low-order eight bits indicate the impact level. Values are: • `0x01` (bit 0) - Source or destination host is in a network monitored by the system. • `0x02` (bit 1) - Source or destination host exists in the network map. • `0x04` (bit 2) - Source or destination host is running a server on the port in the event (if TCP or UDP) or uses the IP protocol. • `0x08` (bit 3) - There is a vulnerability mapped to the operating system of the source or destination host in the event. • `0x10` (bit 4) - There is a vulnerability mapped to the server detected in the event. • `0x20` (bit 5) - The event caused the managed device to drop the session (used only when the device is running in inline, switched, or routed deployment). Corresponds to blocked status in the FireSIGHT System web interface. • `0x40` (bit 6) - The rule that generated this event contains rule metadata setting the impact flag to red. The source or destination host is potentially compromised by a virus, trojan, or other piece of malicious software. • `0x80` (bit 7) - There is a vulnerability mapped to the client detected in the event. (version 5.0+ only) The following impact level values map to specific priorities on the Defense Center. An `X` indicates the value can be 0 or 1: • gray (0, unknown): `00X00000` • red (1, vulnerable): `XXXX1XXX`, `XXX1XXXX`, `X1XXXXXX`, `1XXXXXXX` (version 5.0+ only) • orange (2, potentially vulnerable): `00X0011X` • yellow (3, currently not vulnerable): `00X0001X` • blue (4, unknown target): `00X00001`
Source IP Address	uint8[16]	IP address of the host associated with the impact event. This can contain either an IPv4 or IPv6 address. See IP Addresses, page 1-5 for more information.
Destination IP Address	uint8[16]	IP address of the destination IP address associated with the impact event (if applicable). This can contain either an IPv4 or IPv6 address. See IP Addresses, page 1-5 for more information. This value is `0` if there is no destination IP address.
String Block Type	uint32	Initiates a string data block that contains the impact name. This value is always set to `0`. For more information about string blocks, see String Data Block, page 4-63.

Table 3-5 Impact Event Data Fields (continued)

Field	Data Type	Description
String Block Length	uint32	Number of bytes in the event description string block. This includes the four bytes for the string block type, the four bytes for the string block length, and the number of bytes in the description.
Description	string	Description of the impact event.

User Record

When you request metadata, you can retrieve information about the users referenced in events generated by components in your FireSIGHT System. The eStreamer service transmits metadata containing user information for an event within a User record, the format of which is shown below. The user metadata record can be used to determine a user name associated with an event by correlating the metadata with the user ID value from a User Vulnerability Change Data Block, User Host Deletion Data Block, User Service Deletion Data Block, User Criticality Change Blocks, Attribute Definition Data Block, User Attribute Value Data Block, or Scan Result Data Block. (User information is sent when one of the metadata flags—bits 1, 14, 15, or 20 in the Request Flags field of a request message—is set. See Request Flags, page 2-11.) Note that the Record Type field, which appears after the Message Length field, has a value of `62`, indicating a User record.

Byte	0								1								2								3							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Header Version (1)									Message Type (4)																							
Message Length																																
Record Type (62)																																
Record Length																																
User ID																																
Name Length																																
Name...																																

The following table describes the fields in the User record.

Table 3-6 User Record Fields

Field	Data Type	Description
User ID	uint32	The user ID number.
Name Length	uint32	The number of bytes included in the user name.
Name	string	The name of the user.

Rule Message Record for 4.6.1+

Rule message information for an event is transmitted within a Rule Message record, the format of which is shown below. The eStreamer service transmits the Rule Message record for 4.6.1+ when you request Version 2 or Version 3 metadata. The Rule Message record for 4.6.1+ contains the same fields as the Rule Message record for 4.6 and lower but also has new UUID and Revision UUID fields. (Version 2, Version 3, or Version 4 metadata information is sent when the appropriate metadata flag—bit 14 for Version 2, bit 15 for Version 3, or bit 20 for Version 4 in the Request Flags field of a request message—is set. See Request Flags, page 2-11.) Note that the Record Type field, which appears after the Message Length field, has a value of 66, indicating a Rule Message Version 2 record.

Byte	0								1								2								3							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	Header Version (1)																Message Type (4)															
	Message Length																															
	Record Type (66)																															
	Record Length																															
Signature Key	Generator ID																															
	Rule ID																															
	Revision Number																															
	Rendered Signature ID																															
	Message Length																Rule UUID															
Rule UUID	Rule UUID cont.																															
	Rule UUID cont.																															
	Rule UUID cont.																															
	Rule UUID cont.																Rule Revision UUID															
Rule Revision UUID	Rule Revision UUID cont.																															
	Rule Revision UUID cont.																															
	Rule Revision UUID cont.																															
	Rule Revision UUID cont.																Message...															

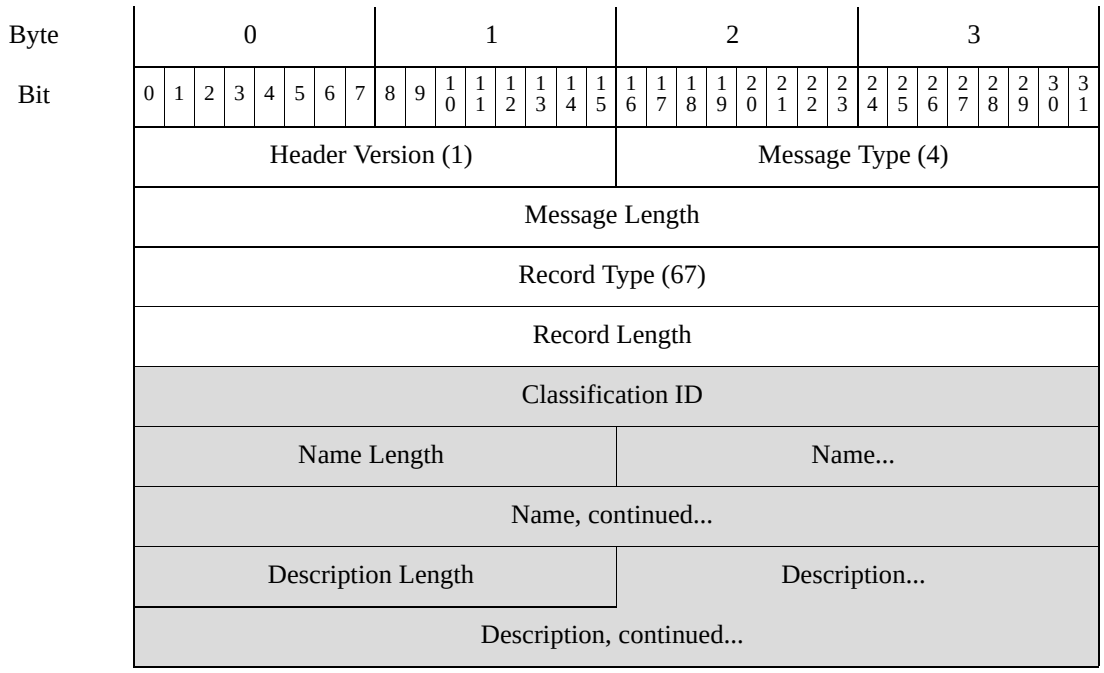
The following table describes each rule-specific field.

Table 3-7 Rule Message Record Fields

Field	Data Type	Description
Generator ID	uint32	The generator identification number.
Rule ID	uint32	The rule identification number for the local computer.
Rule Revision	uint32	The rule revision number. This is currently set to `0` for all rule messages.
Rendered Signature ID	uint32	The rule identification number rendered to the FireSIGHT System interface.
Message Length	uint16	The number of bytes included in the rule text.
UUID	uint8[16]	A rule ID number that acts as a unique identifier for the rule.
Revision UUID	uint8[16]	A rule revision ID number that acts as a unique identifier for the revision.
Message	variable	Rule message that triggered the event.

Classification Record for 4.6.1+

The eStreamer service transmits the classification information for an event in a Classification record for 4.6.1+, the format of which is shown below. The Classification record for 4.6.1+ contains the same fields as the Classification record for 4.6 and lower but also has new UUID and Revision UUID fields. (Classification information is sent when the Version 3 or Version 4 metadata flag—bit 15 or bit 20 in the Request Flags field of a request message—is set. See Request Flags, page 2-11.) Note that the Record Type field, which appears after the Message Length field, has a value of `67`, indicating a Classification Version 2 record.



Byte	0								1								2								3							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Classification UUID	Classification UUID Classification UUID, continued Classification UUID, continued Classification UUID, continued																															
Classification Revision UUID	Classification Revision UUID Classification Revision UUID, continued Classification Revision UUID, continued Classification Revision UUID, continued																															

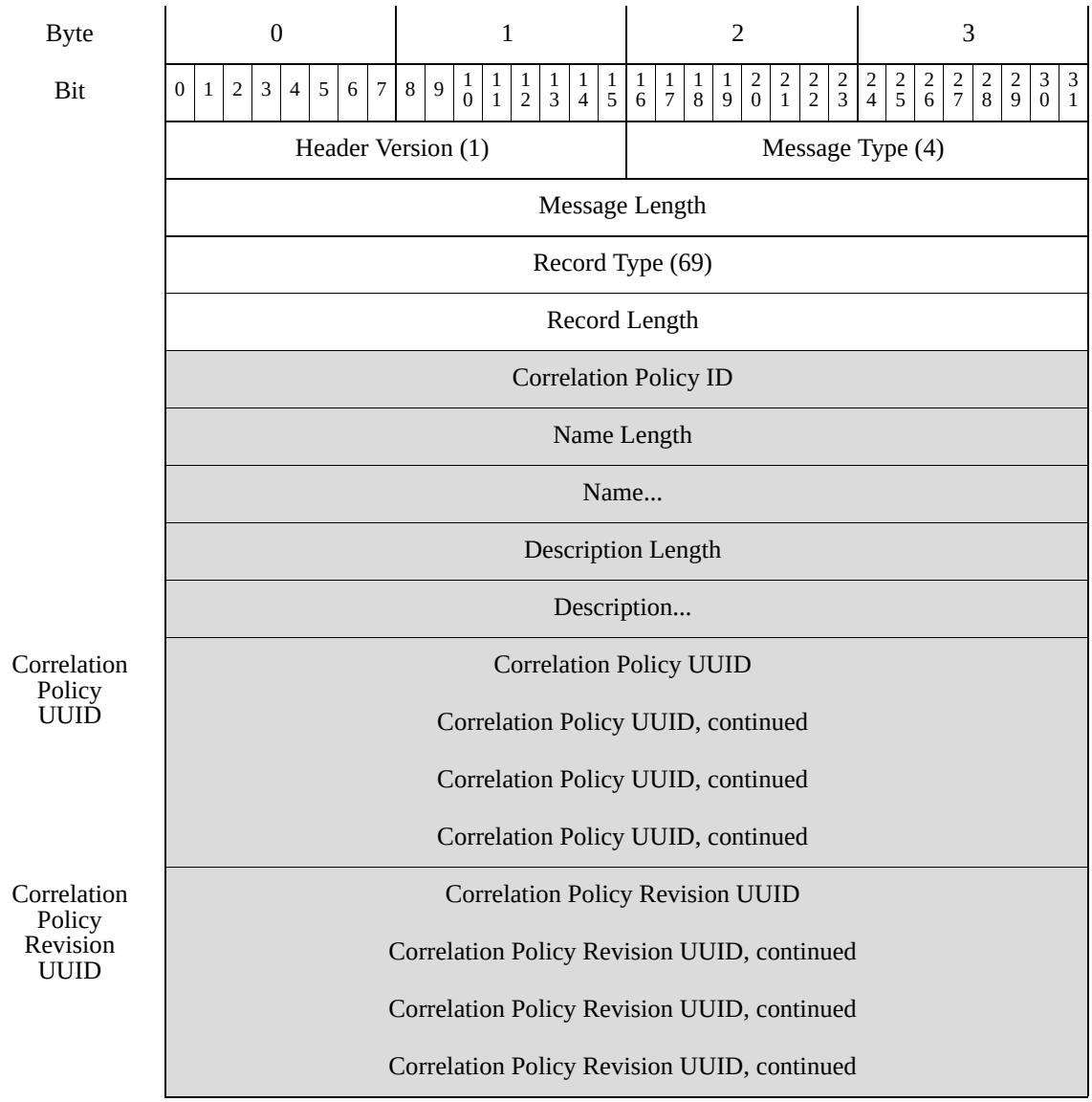
The following table describes the fields in the Classification record.

Table 3-8 Classification Record Fields

Field	Data Type	Description
Classification ID	uint32	The classification ID number.
Name Length	uint16	The number of bytes included in the name.
Name	string	The classification name.
Description Length	uint16	The number of bytes included in the description.
Description	string	The classification description.
UUID	uint8[16]	A classification ID number that acts as a unique identifier for the classification.
Revision UUID	uint8[16]	A classification revision ID number that acts as a unique identifier for the classification revision.

Correlation Policy Record

The eStreamer service transmits metadata containing the correlation policy for a correlation event within a Correlation Policy record, the format of which is shown below. (Correlation policy information is sent when the Version 3 or Version 4 metadata flag—bit 15 or bit 20 in the Request Flags field of a request message—is set. See Request Flags, page 2-11.) Note that the Record Type field, which appears after the Message Length field, has a value of `69`, indicating a Correlation Policy record.



The following table describes the fields in the Correlation Policy record.

Table 3-9 Correlation Policy Record Fields

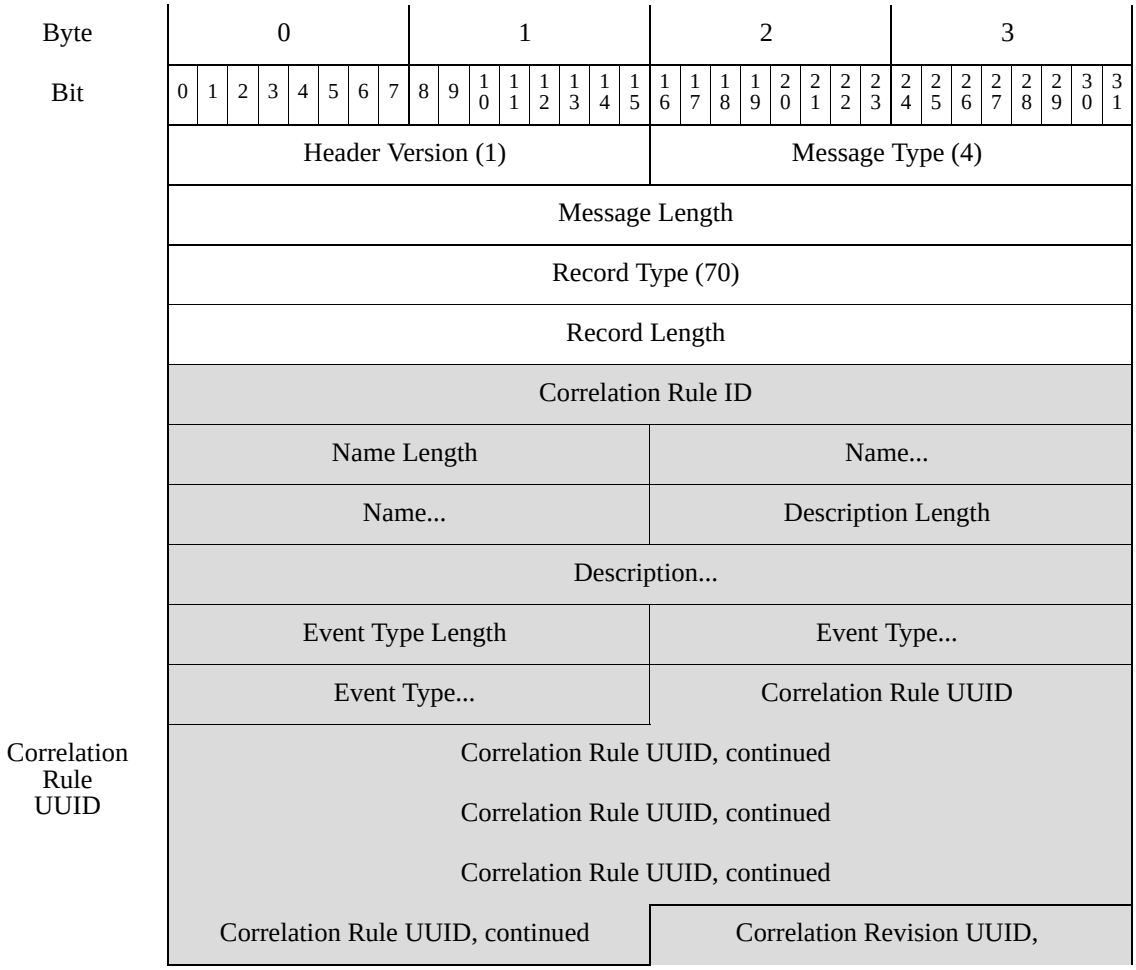
Field	Data Type	Description
Correlation Policy ID	uint32	The correlation policy ID number.
Name Length	uint16	The number of bytes included in the correlation policy name.
Name	string	The name of the correlation policy that triggered the event.
Description Length	uint16	The number of bytes included in the correlation policy description.
Description	string	The description of the correlation policy that triggered the event.

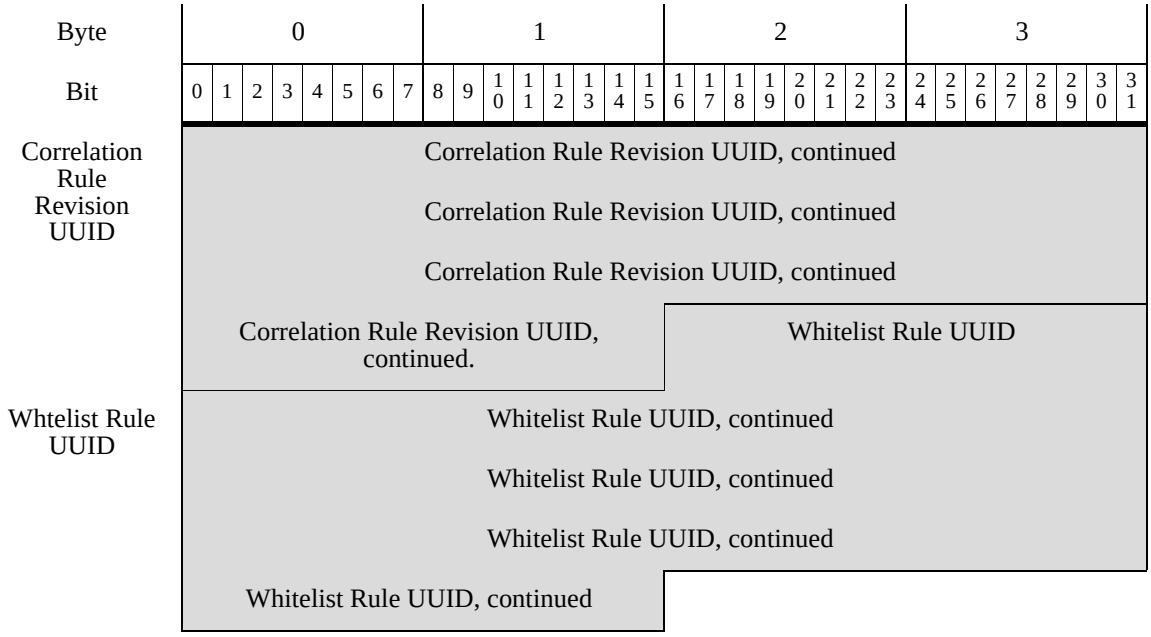
Table 3-9 Correlation Policy Record Fields (continued)

Field	Data Type	Description
UUID	uint8[16]	A correlation policy ID number that acts as a unique identifier for the correlation policy.
Revision UUID	uint8[16]	A correlation policy revision ID number that acts as a unique identifier for the correlation policy.

Correlation Rule Record

The eStreamer service transmits metadata containing information on the correlation rule that triggered a correlation event within a Correlation Rule record, the format of which is shown below. (Correlation rule information is sent when the Version 3 or Version 4 metadata flag—bit 15 or bit 20 in the Request Flags field of a request message—is set. See Request Flags, page 2-11.) Note that the Record Type field, which appears after the Message Length field, has a value of 70, indicating a Correlation Rule record.





The following table describes the fields in the Correlation Rule record.

Table 3-10 Correlation Rule Record Fields

Field	Data Type	Description
Correlation Rule ID	uint32	The correlation rule ID number.
Name Length	uint16	The number of bytes included in the correlation rule name.
Name	string	The name of the correlation rule that triggered the event.
Description Length	uint16	The number of bytes included in the correlation rule description.
Description	string	The description of the correlation rule that triggered the event.
Event Type Length	uint16	The number of bytes included in the event type description.
Event Type	string	The description of the event that triggered the correlation rule.
UUID	uint8[16]	A correlation rule ID number that acts as a unique identifier for the correlation rule.
Revision UUID	uint8[16]	A correlation rule revision ID number that acts as a unique identifier for the correlation rule revision.
Whitelist UUID	uint8[16]	A correlation ID number that acts as a unique identifier for the event sent as a result of a whitelist violation.

Intrusion Event Extra Data Record

The eStreamer service transmits the event extra data associated with an intrusion event in the Intrusion Event Extra Data record. The record type is always `110`.

The event extra data appears in an encapsulated Event Extra Data data block, which always has a data block type value of `4`. (The Event Extra Data data block is a series 2 data block. For more information about series 2 data blocks, see Understanding Series 2 Data Blocks, page 3-44.)

The supported types of extra data include IPv6 source and destination addresses, as well as the originating IP addresses (v4 or v6) of clients connecting to a web server through an HTTP proxy or load balancer. The graphic below shows the format of the Intrusion Event Extra Data record.

If bit 27 is set in the Request Flags field of the request message, you receive the event extra data for each intrusion event. If you set bit 20, you also receive the event extra data metadata described in Intrusion Event Extra Data Metadata, page 3-23. If you enable bit 23, eStreamer will include the extended event header. See Request Flags, page 2-11 for information on setting request flags.

Byte	0								1								2								3							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Header Version (1)																	Message Type (4)															
Message Length																																
Record Type (110)																																
Record Length																																
eStreamer Server Timestamp (in events, only if bit 23 is set)																																
Reserved for Future Use (in events, only if bit 23 is set)																																
Event Extra Data Data Block Type (4)																																
Event Extra Data Data Block Length																																
Device ID																																
Event ID																																
Event Second																																
Type																																
BLOB Block Type (1)																																
BLOB Length																																
Event Extra Data																																

Note that the Event Extra Data block structure includes a BLOB block type, which is one of several variable length data structures introduced in Version 4.10 of the FireSIGHT System.

The following table describes the fields in the Intrusion Event Extra Data record.

Table 3-11 Intrusion Event Extra Data Data Block Fields

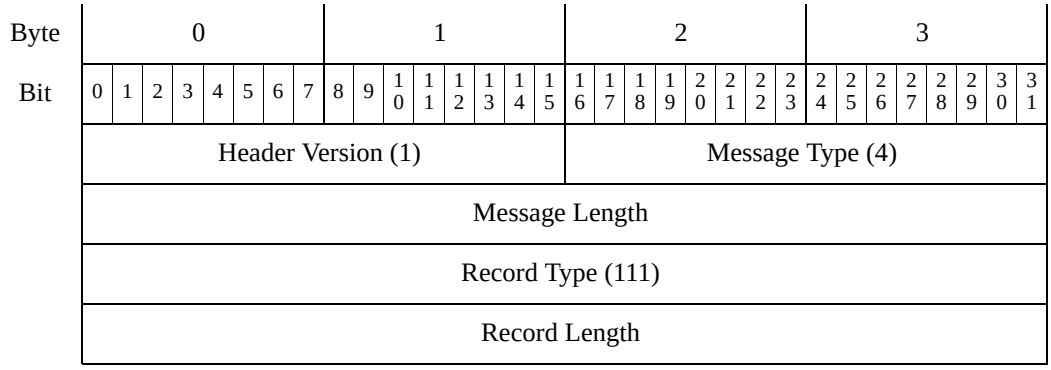
Field	Data Type	Description
Event Extra Data Data Block Type	uint32	Initiates an Event Extra Data data block. This value is always 4. The block type is a series 2 block; for information see Understanding Series 2 Data Blocks, page 3-44.
Event Extra Data Data Block Length	uint32	Length of the data block. Includes the number of bytes of data plus the 8 bytes in the two data block header fields.
Device ID	uint32	The managed device identification number.
Event ID	uint32	The event identification number.
Event Second	uint32	UNIX timestamp of the event (seconds since 01/01/1970).
Type	uint32	Identifier for the type of extra data; for example: • 1 - XFF client (IPv4) • 2 - XFF client (IPv6) • 9 - HTTP URI
BLOB Block Type	uint32	Initiates a BLOB data block containing extra data. This value is always 1. The block type is a series 2 block.
Length	uint32	Total number of bytes in the BLOB data block.
Extra Data	variable	The content of the extra data. The data type is indicated in the Type field.

Intrusion Event Extra Data Metadata

The eStreamer service transmits the event extra data metadata associated with intrusion event extra data records in the Intrusion Event Extra Data Metadata record. The record type is always 111.

The event extra data metadata appears in an encapsulated Event Extra Data Metadata data block, which always has a data block type value of 5. The Event Extra Data data block is a series 2 data block.

If bit 20 is set in the Request Flags field of a request message, you receive the event extra data metadata. If you want to receive both intrusion events and event extra data metadata, you must set bit 2 as well. See Request Flags, page 2-11. If you enable bit 23, an extended event header is included in the record.



Byte	0								1								2								3							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
eStreamer Server Timestamp (in events, only if bit 23 is set)																																
Reserved for Future Use (in events, only if bit 23 is set)																																
Event Extra Data Metadata Data Block Type (5)																																
Data Block Length																																
Type																																
String Block Type (0)																																
String Block Length																																
Name...																																
String Block Type (0)																																
String Block Length																																
Encoding																																

Note that the block structure includes encapsulated String block types, one of several series 2 variable length data structures introduced in Version 4.10 of the FireSIGHT System.

The following table describes the fields in the Event Extra Data Metadata record.

Table 3-12 Event Extra Data Metadata Data Block Fields

Field	Data Type	Description
Event Extra Data Metadata Data Block Type	uint32	Initiates an Event Extra Data Metadata data block. This value is always `5`. This block type is a series 2 block.
Event Extra Data Metadata Data Block Length	uint32	Length of the data block. Includes the number of bytes of data plus the 8 bytes in the two data block header fields.
Type	uint32	The type of extra data. Matches the Type field in the associated Event Extra Data record.
String Block Type	uint32	Initiates a String data block for the client application version. This value is always `0`. This block type is a series 2 block.
String Block Length	uint32	Number of bytes in the client application version String data block, including eight bytes for the string block type and length fields, plus the number of bytes in the version string.
Name	string	Name of the type of event extra data, for example, XFF client (IPv6), and HTTP URI.
String Block Type	uint32	Initiates a string data block for the client application URL. This value is always `0`. This block type is a series 2 block.

Table 3-12 Event Extra Data Metadata Data Block Fields (continued)

Field	Data Type	Description
String Block Length	uint32	Number of bytes in the client application URL String data block, including eight bytes for the string block type and length fields, plus the number of bytes in the URL string.
Encoding	string	Encoding used for the event extra data, for example, IPv4, IPv6, or string.

Security Zone Name Record

The eStreamer service transmits metadata containing information on the name of the security zone associated with an intrusion event or connection event within a Security Zone Name record, the format of which is shown below. (Security zone information is sent when the Version 4 metadata flag—bit 20 in the Request Flags field of a request message—is set. See Request Flags, page 2-11.) Note that the Record Type field, which appears after the Message Length field, has a value of `115`, indicating a Security Zone Name record. It contains a UUID String data block, block type 14 in the series 2 set of data blocks.

Byte	0								1								2								3							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Header Version (1)																	Message Type (4)															
Message Length																																
Record Type (115)																																
Record Length																																
Security Zone Name Data Block (14)																																
Security Zone Name Data Block Length																																
Security Zone UUID																																
String Block Type (0)																																
String Block Length																																
Security Zone Name...																																

The following table describes the fields in the Security Zone Name data block.

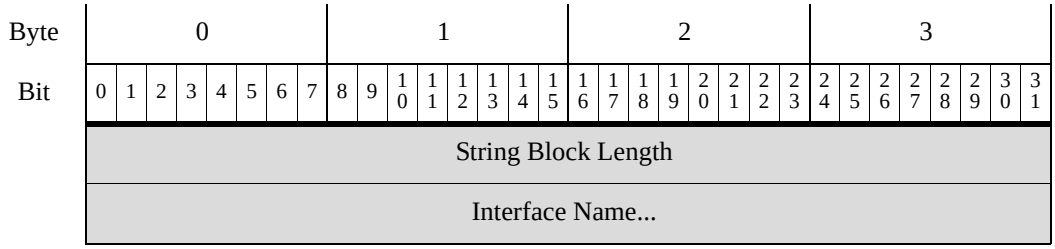
Table 3-13 Security Zone Name Data Block Fields

Field	Data Type	Description
Security Zone Name Data Block Type	uint32	Initiates a Security Zone Name data block. This value is always 14. The block type is a series 2 block.
Security Zone Name Data Block Length	uint32	Length of the data block. Includes the number of bytes of data plus the 8 bytes in the two data block header fields.
Security Zone UUID	uint8[16]	The unique identifier for the security zone associated with the connection event.
String Block Type	uint32	Initiates a String data block containing the name of the security zone. This value is always 0.
String Block Length	uint32	The number of bytes included in the security zone name String data block, including eight bytes for the block type and header fields plus the number of bytes in the name.
Security Zone Name	string	The security zone name.

Interface Name Record

The eStreamer service transmits metadata containing information on the name of the interface associated with an intrusion event or connection event within an Interface Name record, the format of which is shown below. (Interface name information is sent when the Version 4 metadata flag—bit 20 in the Request Flags field of a request message—is set. See Request Flags, page 2-11.) Note that the Record Type field, which appears after the Message Length field, has a value of 116, indicating an Interface Name record. It contains a UUID String data block, block type 14 in the series 2 set of data blocks.

Byte	0								1								2								3							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Header Version (1)																	Message Type (4)															
Message Length																																
Record Type (116)																																
Record Length																																
Interface Name Data Block (14)																																
Interface Name Data Block Length																																
Interface UUID																																
String Block Type (0)																																



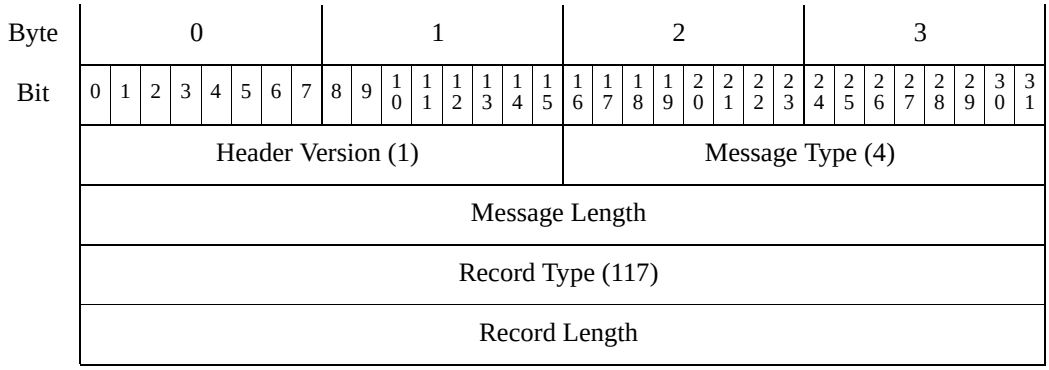
The following table describes the fields in the Interface Name data block.

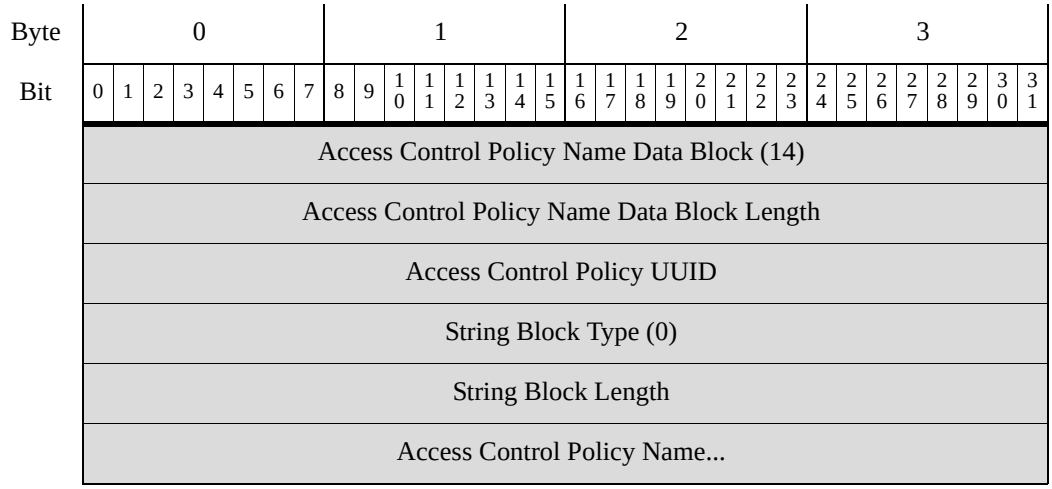
Table 3-14 Interface Name Data Block Fields

Field	Data Type	Description
Interface Name Data Block Type	uint32	Initiates an Interface Name data block. This value is always `14`. The block type is a series 2 block.
Interface Name Data Block Length	uint32	Length of the data block. Includes the number of bytes of data plus the 8 bytes in the two data block header fields.
Interface UUID	uint8[16]	An interface ID number that acts as a unique identifier for the interface associated with the connection event.
String Block Type	uint32	Initiates a String data block containing the name of the interface. This value is always `0`.
String Block Length	uint32	The number of bytes included in the interface name String data block, including eight bytes for the block type and header fields plus the number of bytes in the interface name.
Interface Name	string	The interface name.

Access Control Policy Name Record

The eStreamer service transmits metadata on the name of the access control policy that triggered an intrusion event or connection event within an Access Control Policy Name record, the format of which is shown below. (Access control policy name information is sent when the Version 4 metadata flag—bit 20 in the Request Flags field of a request message—is set. See Request Flags, page 2-11.) Note that the Record Type field, which appears after the Message Length field, has a value of `117`, indicating an Access Control Policy Name record. It contains a UUID String data block, block type 14 in the series 2 set of data blocks.





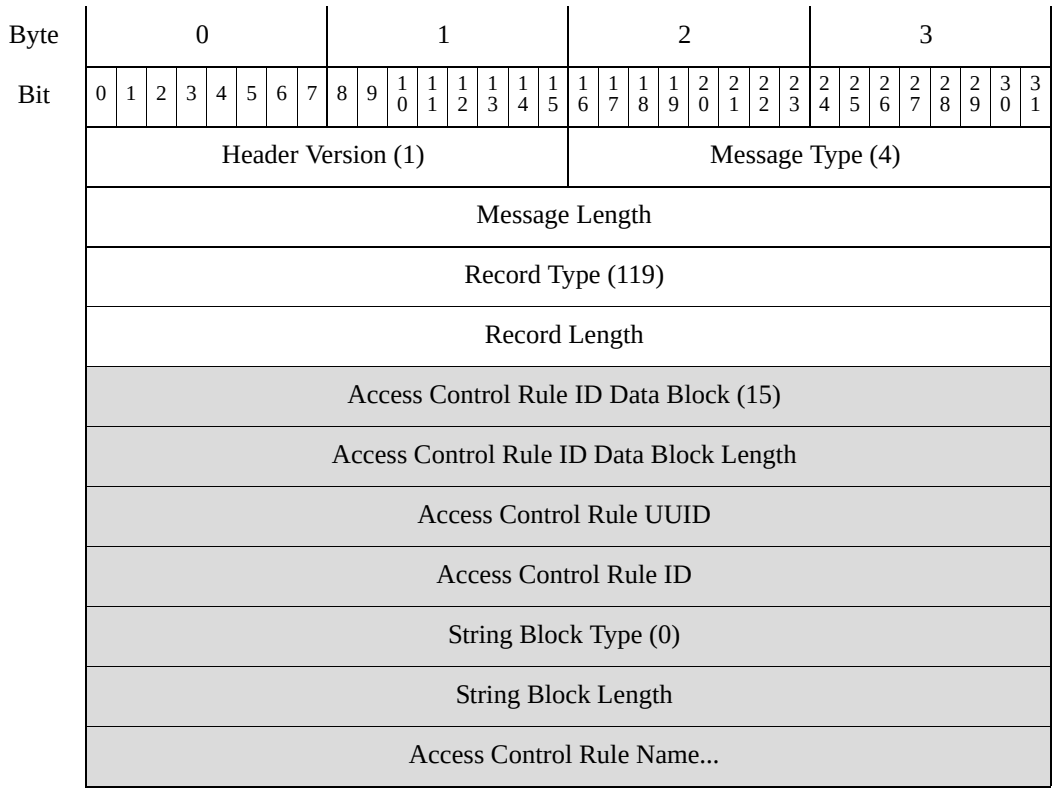
The following table describes the fields in the Access Control Policy Name data block.

Table 3-15 Access Control Policy Name Data Block Fields

Field	Data Type	Description
Access Control Policy Name Data Block Type	uint32	Initiates an Access Control Policy Name data block. This value is always `14`. The block type is a series 2 block.
Access Control Policy Name Data Block Length	uint32	Length of the data block. Includes the number of bytes of data plus the 8 bytes in the two data block header fields.
Access Control Policy UUID	uint8[16]	An ID number that acts as a unique identifier for the access control policy associated with the intrusion event or connection event
String Block Type	uint32	Initiates a String data block containing the name of the access control policy. This value is always `0`.
String Block Length	uint32	The number of bytes included in the access control policy name String data block, including eight bytes for the block type and header fields plus the number of bytes in the access control policy name.
Access Control Policy Name	string	The access control policy name.

Access Control Rule ID Record Metadata

The eStreamer service transmits metadata containing information about the access control rule that triggered an intrusion event or connection event within an Access Control Rule ID record, the format of which is shown below. Access control rule metadata is sent when the Version 4 metadata flag—bit 20 in the Request Flags field of a request message—is set. See Request Flags, page 2-11.) Note that the Record Type field, which appears after the Message Length field, has a value of `119`, indicating an Access Control Rule ID record. It contains a Rule ID data block, block type 15 in the series 2 set of data blocks.



The following table describes the fields in the Access Control Rule ID data block.

Table 3-16 Access Control Rule ID Data Block Fields

Field	Data Type	Description
Access Control Rule ID Data Block Type	uint32	Initiates an Access Control Rule ID data block. This value is always `15`. The block type is a series 2 block.
Access Control Rule ID Data Block Length	uint32	Length of the data block. Includes the number of bytes of data plus the 8 bytes in the two data block header fields.
Access Control Rule UUID	uint8[16]	A rule ID that acts as the unique identifier for the rule in the access control policy associated with the connection event.
Access Control Rule ID	uint32	The internal identifier for the rule in the access control policy associated with the connection event.
String Block Type	uint32	Initiates a String data block containing the name of the access control rule. This value is always `0`.
String Block Length	uint32	The number of bytes included in the String data block, including eight bytes for the block type and header fields plus the number of bytes in the rule name.
Access Control Rule Name	string	The access control rule name.

Managed Device Record Metadata

The eStreamer service transmits metadata containing information on the managed device associated with an intrusion event within a Managed Device record, the format of which is shown below. Managed device metadata is sent when the Version 4 metadata flag—bit 20 in the Request Flags field of a request message—is set. See Request Flags, page 2-11.) Note that the Record Type field, which appears after the Message Length field, has a value of `123`, indicating a Managed Device record.

Byte	0								1								2								3							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	Header Version (1)																Message Type (4)															
	Message Length																															
	Record Type (123)																															
	Record Length																															
	Device ID																															
	Name Length																															
	Name...																															

The following table describes the fields in the Managed Device record.

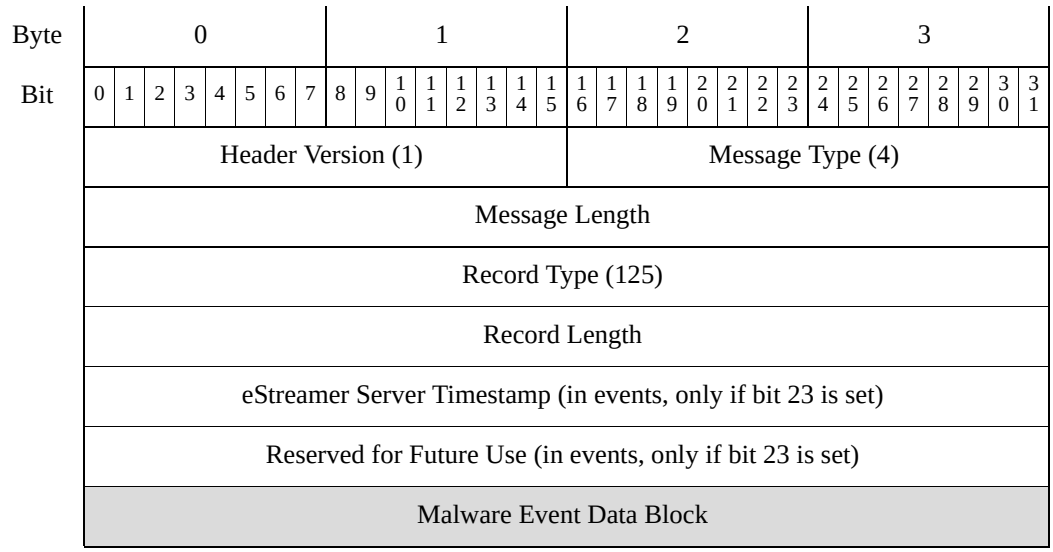
Table 3-17 Managed Device Record Fields

Field	Data Type	Description
Device ID	uint32	ID number of the managed device.
Name Length	uint32	The number of bytes included in the name.
Name	string	The managed device name.

Malware Event Record 5.1.1+

The fields in the malware event record are shaded in the following graphic. The record type is 125.

You request malware event records by setting the malware event flag—bit 30 in the Request Flags field—in the request message with an event version of `2` and an event code of `101`. See Request Flags, page 2-11. If you enable bit 23, an extended event header is included in the record. It contains a Malware Event data block, one of block types 24, 33, 35, 44, or 47 in the series 2 set of data blocks.



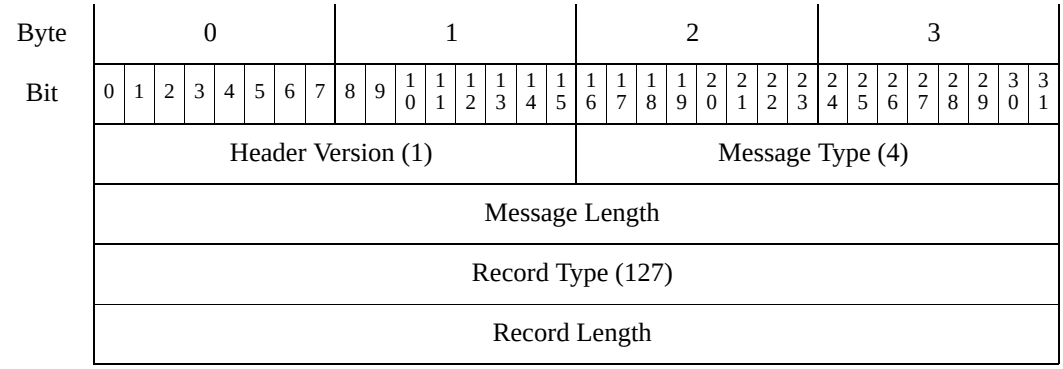
The following table describes each malware event record data field.

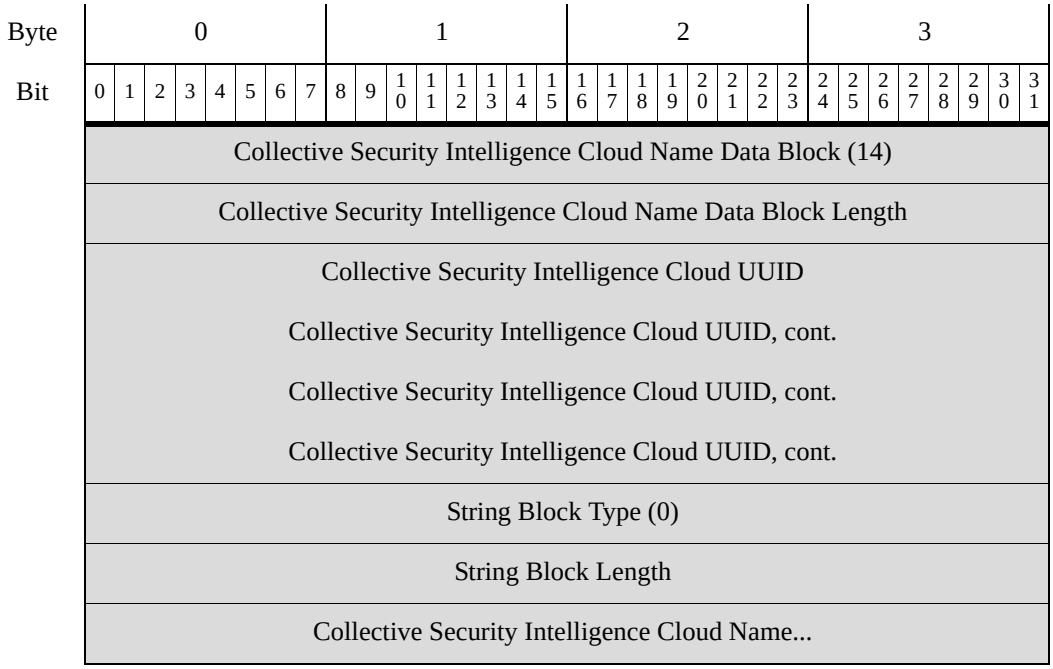
Table 3-18 Malware Event Record Fields

Field	Data Type	Description
Malware Event Data Block	variable	Indicates a malware event data block. See Malware Event Data Block 5.3.1+, page 3-64 for more information.

Collective Security Intelligence Cloud Name Metadata

The eStreamer service transmits metadata containing information on the name of the Collective Security Intelligence Cloud (referred to as the Cisco cloud or simply cloud) associated with an intrusion event or connection event within a Collective Security Intelligence Cloud Name record, the format of which is shown below. (Cisco cloud name information is sent when the Version 4 metadata flag—bit 20 in the Request Flags field of a request message—is set. See Request Flags, page 2-11.) Note that the Record Type field, which appears after the Message Length field, has a value of `127`, indicating a Collective Security Intelligence Cloud Name record. It contains a UUID String data block, block type 14 in the series 2 set of data blocks.





The following table describes the fields in the Collective Security Intelligence Cloud Name data block.

Table 3-19 Collective Security Intelligence Cloud Name Data Block Fields

Field	Data Type	Description
Collective Security Intelligence Cloud Name Data Block Type	uint32	Initiates a Collective Security Intelligence Cloud Name data block. This value is always `14`. The block type is a series 2 block.
Collective Security Intelligence Cloud Name Data Block Length	uint32	Length of the data block. Includes the number of bytes of data plus the 8 bytes in the two data block header fields.
Collective Security Intelligence Cloud UUID	uint8[16]	A Collective Security Intelligence Cloud ID number that acts as a unique identifier for the Collective Security Intelligence Cloud associated with the connection event.
String Block Type	uint32	Initiates a String data block containing the name of the Collective Security Intelligence Cloud. This value is always `0`.

Table 3-19 Collective Security Intelligence Cloud Name Data Block Fields (continued)

Field	Data Type	Description
String Block Length	uint32	The number of bytes included in the Collective Security Intelligence Cloud Name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Collective Security Intelligence Cloud name.
Collective Security Intelligence Cloud Name	string	The Collective Security Intelligence Cloud name.

Malware Event Type Metadata

The eStreamer service transmits metadata containing malware event type information for an event within a malware event type record, the format of which is shown below. (Malware event type information is sent when the metadata flag, bit 20 in the request flags field of a request message, is set. See Request Flags, page 2-11.) Note that the record type field, which appears after the message length field, has a value of `128`, indicating a malware event type record.

Byte	0								1								2								3							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Header Version (1)									Message Type (4)																							
Message Length																																
Record Type (128)																																
Record Length																																
Malware Event Type ID																																
Malware Event Type Length																																
Malware Event Type...																																

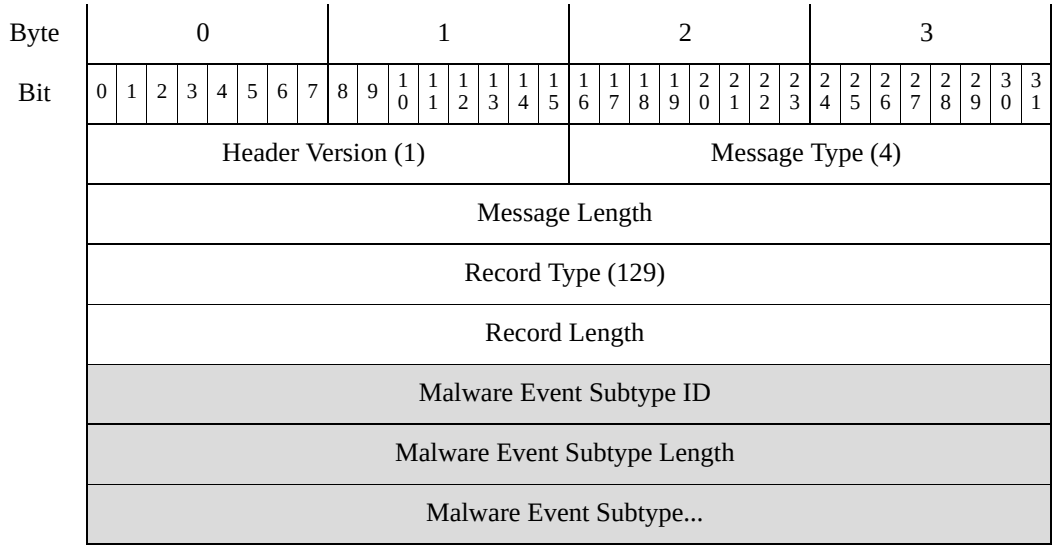
The following table describes the fields in the malware event type record.

Table 3-20 Malware Event Type Record Fields

Field	Data Type	Description
Malware Event Type ID	uint32	The malware event type ID number.
Malware Event Type Length	uint32	The number of bytes included in the malware event type.
Malware Event Type	string	The type of malware event.

Malware Event Subtype Metadata

The eStreamer service transmits metadata containing malware event subtype information for an event within a malware event subtype record, the format of which is shown below. (Malware event type information is sent when the metadata flag, bit 20 in the request flags field of a request message, is set. See Request Flags, page 2-11.) Note that the record type field, which appears after the message length field, has a value of `129`, indicating a malware event subtype record.



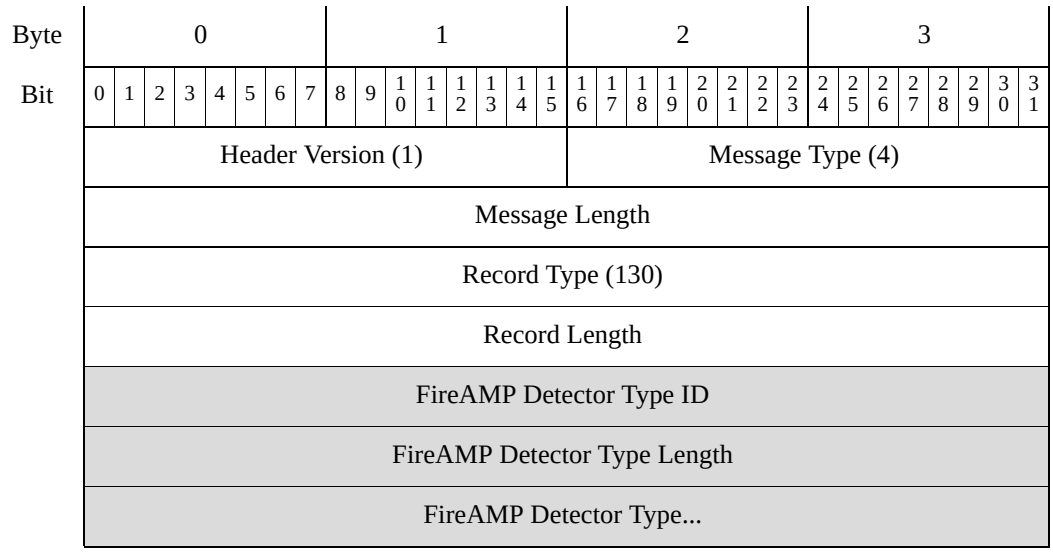
The following table describes the fields in the malware event subtype record.

Table 3-21 Malware Event Subtype Record Fields

Field	Data Type	Description
Malware Event Subtype ID	uint32	The malware event subtype ID number.
Malware Event Subtype Length	uint32	The number of bytes included in the malware event subtype.
Malware Event Subtype	string	The malware event subtype.

FireAMP Detector Type Metadata

The eStreamer service transmits metadata containing FireAMP detector type information for an event within a FireAMP Detector Type record, the format of which is shown below. (FireAMP detector type information is sent when one of the metadata flags—bits 1, 14, 15, or 20 in the Request Flags field of a request message—is set. See Request Flags, page 2-11.) Note that the Record Type field, which appears after the Message Length field, has a value of `130`, indicating a FireAMP detector type record.



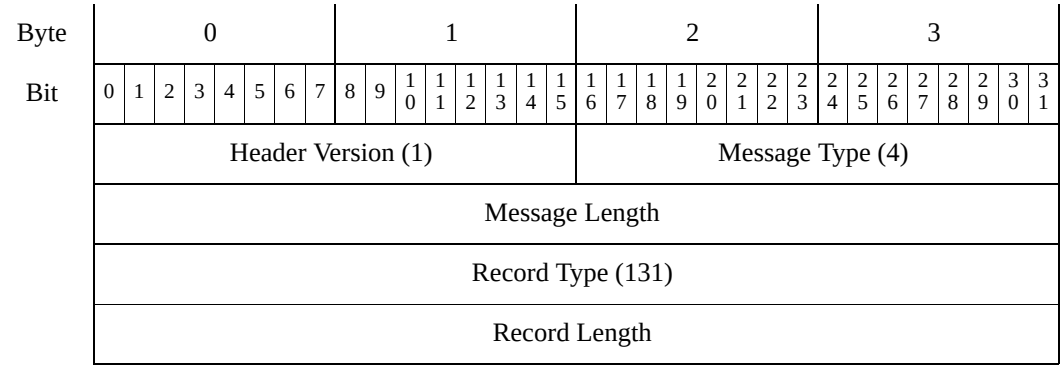
The following table describes the fields in the FireAMP Detector Type record.

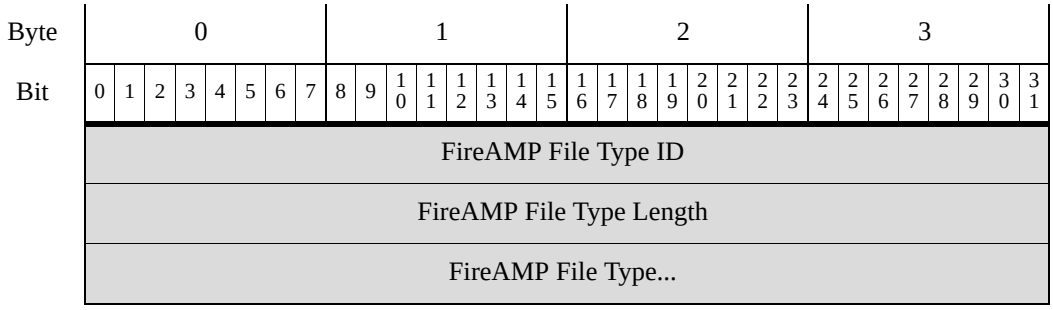
Table 3-22 FireAMP Detector Type Record Fields

Field	Data Type	Description
FireAMP Detector Type ID	uint32	The FireAMP detector type ID number.
FireAMP Detector Type Length	uint32	The number of bytes included in the FireAMP detector type.
FireAMP Detector Type	string	The type of FireAMP detector.

FireAMP File Type Metadata

The eStreamer service transmits metadata containing FireAMP file type information for an event within a FireAMP File Type record, the format of which is shown below. (FireAMP file type information is sent when one of the metadata flags—bits 1, 14, 15, or 20 in the Request Flags field of a request message—is set. See Request Flags, page 2-11.) Note that the Record Type field, which appears after the Message Length field, has a value of `131`, indicating a FireAMP file type record.





The following table describes the fields in the FireAMP File Type record.

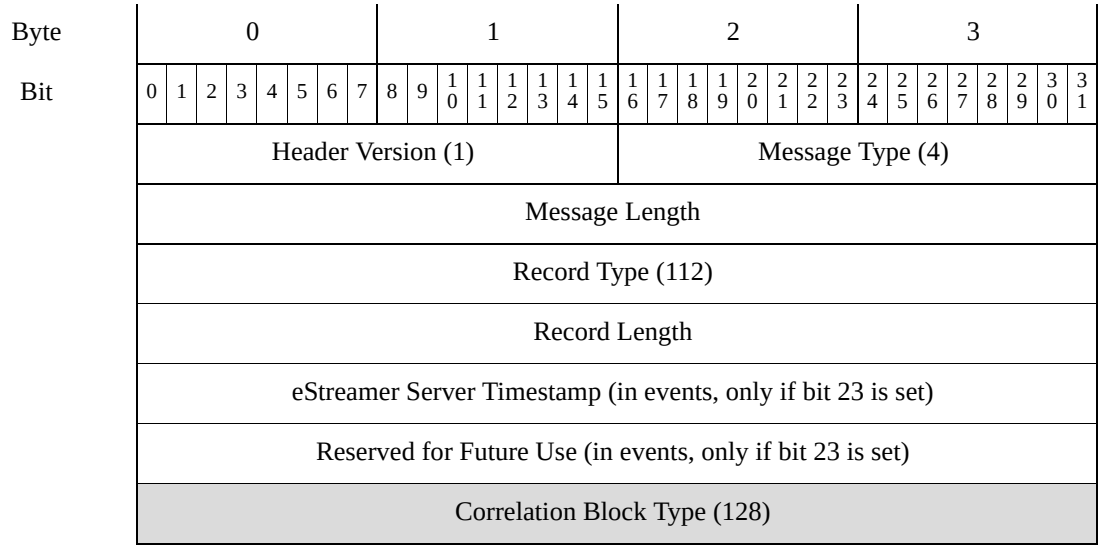
Table 3-23 FireAMP File Type Record Fields

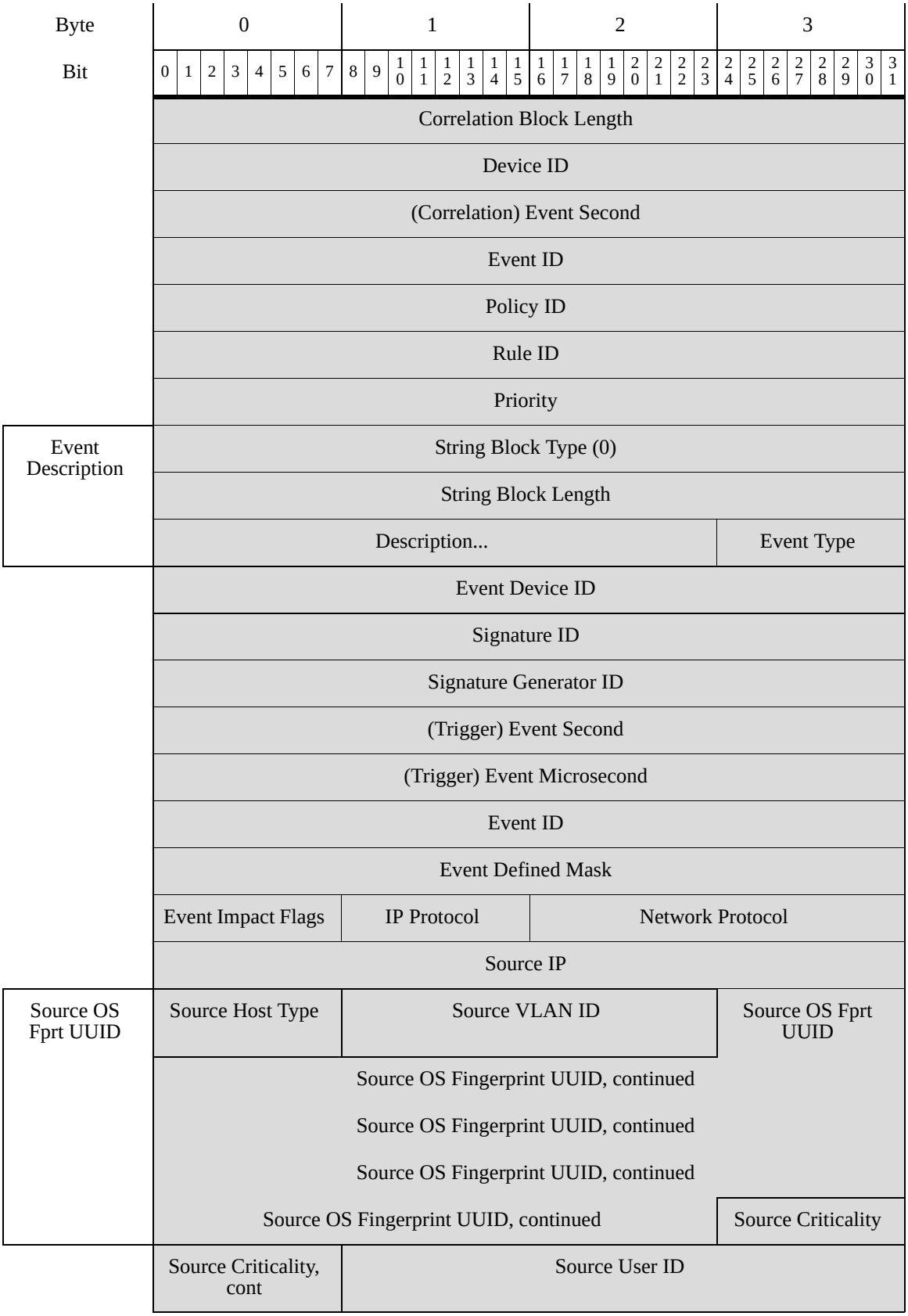
Field	Data Type	Description
FireAMP File Type ID	uint32	The FireAMP file type ID number.
FireAMP File Type Length	uint32	The number of bytes included in the FireAMP file type.
FireAMP File Type	string	The type of detected file.

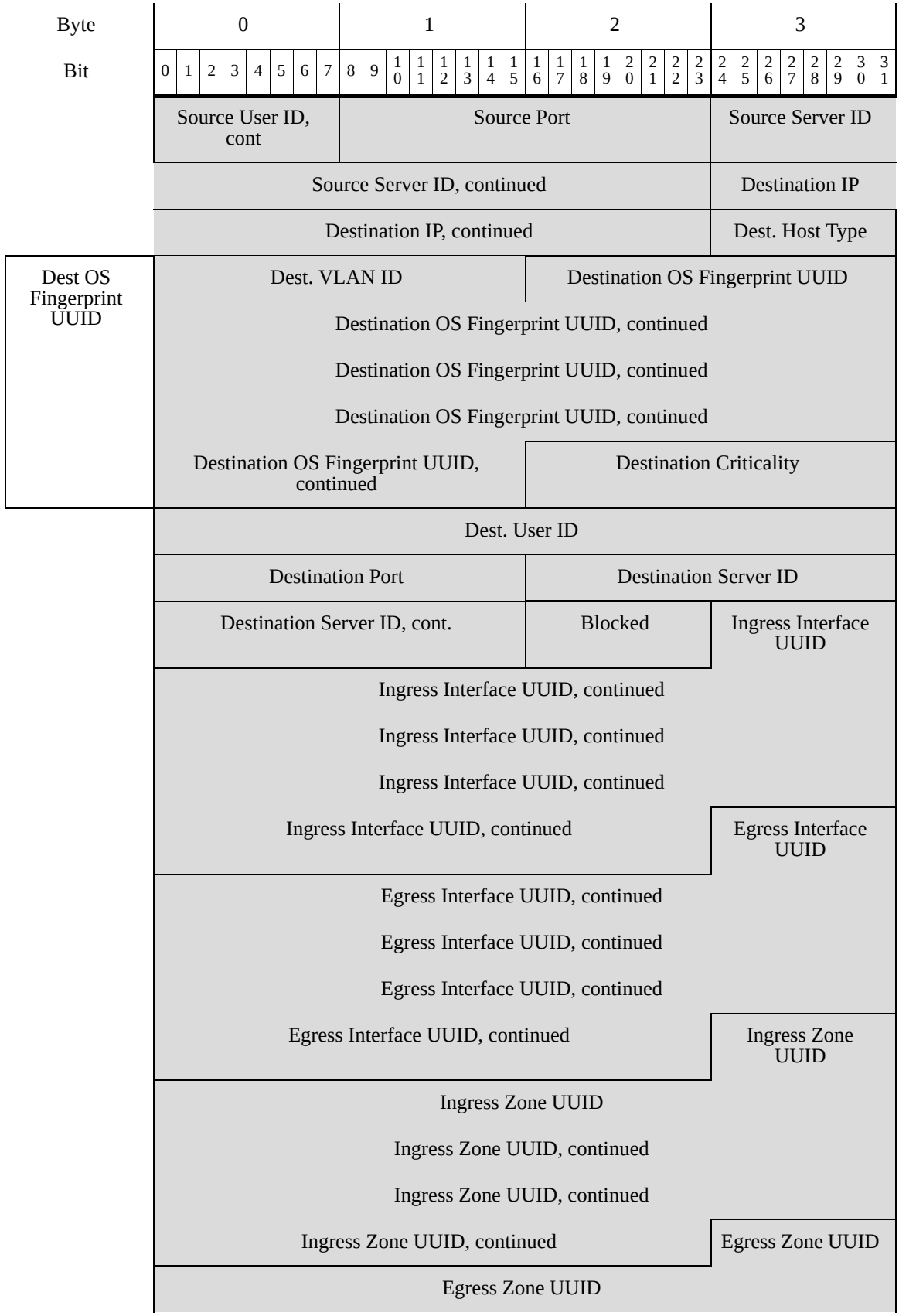
Correlation Event for 5.1+

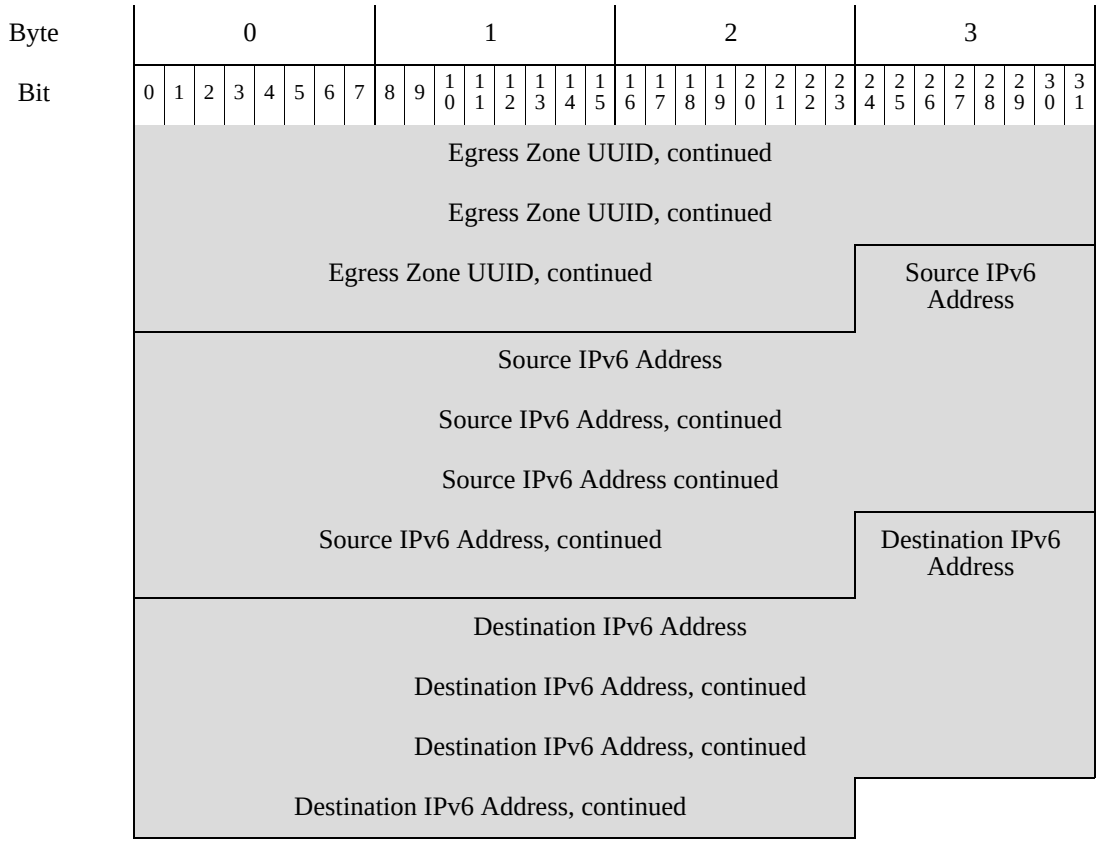
Correlation events (called compliance events in pre-5.0 versions) contain information about correlation policy violations. This message uses the standard eStreamer message header and specifies a record type of 112, followed by a correlation data block of type 128 in the series 1 set of data blocks. Data block type 128 differs from its predecessor (block type 116) in including IPv6 support.

You can request 5.1+ correlation events from eStreamer only by extended request, for which you request event type code `31` and version code `8` in the Stream Request message (see Submitting Extended Requests, page 2-4 for information about submitting extended requests). You can optionally enable bit 23 in the flags field of the initial event stream request message, to include the extended event header. You can also enable bit 20 in the flags field to include user metadata.




Byte
0
1
2
3
Bit
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Correlation Block Length
Device ID
(Correlation) Event Second
Event ID
Policy ID
Rule ID
Priority
Event Description
String Block Type (0)
String Block Length
Description...
Event Type
Event Device ID
Signature ID
Signature Generator ID
(Trigger) Event Second
(Trigger) Event Microsecond
Event ID
Event Defined Mask
Event Impact Flags
IP Protocol
Network Protocol
Source IP
Source OS Fprt UUID
Source Host Type
Source VLAN ID
Source OS Fprt UUID
Source OS Fingerprint UUID, continued
Source OS Fingerprint UUID, continued
Source OS Fingerprint UUID, continued
Source OS Fingerprint UUID, continued
Source Criticality
Source Criticality, cont
Source User ID


Byte
0
1
2
3
Bit
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Source User ID, cont
Source Port
Source Server ID
Source Server ID, continued
Destination IP
Destination IP, continued
Dest. Host Type
Dest OS Fingerprint UUID
Dest. VLAN ID
Destination OS Fingerprint UUID
Destination OS Fingerprint UUID, continued
Destination OS Fingerprint UUID, continued
Destination OS Fingerprint UUID, continued
Destination OS Fingerprint UUID, continued
Destination Criticality
Dest. User ID
Destination Port
Destination Server ID
Destination Server ID, cont.
Blocked
Ingress Interface UUID
Ingress Interface UUID, continued
Ingress Interface UUID, continued
Ingress Interface UUID, continued
Ingress Interface UUID, continued
Egress Interface UUID
Egress Interface UUID, continued
Egress Interface UUID, continued
Egress Interface UUID, continued
Egress Interface UUID, continued
Ingress Zone UUID
Ingress Zone UUID
Ingress Zone UUID, continued
Ingress Zone UUID, continued
Ingress Zone UUID, continued
Egress Zone UUID
Egress Zone UUID



Note that the record structure includes a String block type, which is a block in series 1. For information about series 1 blocks, see Understanding Discovery (Series 1) Blocks, page 4-55.

Table 3-24 Correlation Event 5.1+ Data Fields

Field	Data Type	Description
Correlation Block Type	uint32	Indicates a correlation event data block follows. This field always has a value of `128`. See Understanding Discovery (Series 1) Blocks, page 4-55.
Correlation Block Length	uint32	Length of the correlation data block, which includes 8 bytes for the correlation block type and length plus the correlation data that follows.
Device ID	uint32	Internal identification number of the managed device or Defense Center that generated the correlation event. A value of `0` indicates the Defense Center. You can obtain managed device names by requesting Version 3 metadata. See Managed Device Record Metadata, page 3-30 for more information.
(Correlation) Event Second	uint32	UNIX timestamp indicating the time that the correlation event was generated (in seconds from 01/01/1970).
Event ID	uint32	Correlation event identification number.
Policy ID	uint32	Identification number of the correlation policy that was violated. See Server Record, page 4-14 for information about how to obtain policy identification numbers from the database.

Table 3-24 Correlation Event 5.1+ Data Fields (continued)

Field	Data Type	Description
Rule ID	uint32	Identification number of the correlation rule that triggered to violate the policy. See Server Record, page 4-14 for information about how to obtain policy identification numbers from the database.
Priority	uint32	Priority assigned to the event. This is an integer value from `0` to `5`.
String Block Type	uint32	Initiates a string data block that contains the correlation violation event description. This value is always set to `0`. For more information about string blocks, see String Data Block, page 4-63.
String Block Length	uint32	Number of bytes in the event description string block, which includes four bytes for the string block type and four bytes for the string block length, plus the number of bytes in the description.
Description	string	Description of the correlation event.
Event Type	uint8	Indicates whether the correlation event was triggered by an intrusion, host discovery, or user event: • `1` - intrusion • `2` - host discovery • `3` - user
Event Device ID	uint32	Identification number of the device that generated the event that triggered the correlation event. You can obtain device name by requesting Version 3 metadata. See Managed Device Record Metadata, page 3-30 for more information.
Signature ID	uint32	If the event was an intrusion event, indicates the rule identification number that corresponds with the event. Otherwise, the value is `0`.
Signature Generator ID	uint32	If the event was an intrusion event, indicates the ID number of the FireSIGHT System preprocessor or rules engine that generated the event.
(Trigger) Event Second	uint32	UNIX timestamp indicating the time of the event that triggered the correlation policy rule (in seconds from 01/01/1970).
(Trigger) Event Microsecond	uint32	Microsecond (one millionth of a second) increment that the event was detected.
Event ID	uint32	Identification number of the event generated by the Cisco device.
Event Defined Mask	bits[32]	Set bits in this field indicate which of the fields that follow in the message are valid. See Table 3-25 on page 3-43 for a list of each bit value.

Table 3-24 Correlation Event 5.1+ Data Fields (continued)

Field	Data Type	Description
Event Impact Flags	bits[8]	Impact flag value of the event. The low-order eight bits indicate the impact level. Values are: • `0x01` (bit 0) - Source or destination host is in a network monitored by the system. • `0x02` (bit 1) - Source or destination host exists in the network map. • `0x04` (bit 2) - Source or destination host is running a server on the port in the event (if TCP or UDP) or uses the IP protocol. • `0x08` (bit 3) - There is a vulnerability mapped to the operating system of the source or destination host in the event. • `0x10` (bit 4) - There is a vulnerability mapped to the server detected in the event. • `0x20` (bit 5) - The event caused the managed device to drop the session (used only when the device is running in inline, switched, or routed deployment). Corresponds to blocked status in the FireSIGHT System web interface. • `0x40` (bit 6) - The rule that generated this event contains rule metadata setting the impact flag to red. The source or destination host is potentially compromised by a virus, trojan, or other piece of malicious software. • `0x80` (bit 7) - There is a vulnerability mapped to the client detected in the event. (version 5.0+ only) The following impact level values map to specific priorities on the Defense Center. An `x` indicates the value can be `0` or `1`: • gray (0, unknown): `00X00000` • red (1, vulnerable): `XXXX1XXX, XXX1XXXX, X1XXXXXX, 1XXXXXXX` (Version 5.0+ only) • orange (2, potentially vulnerable): `00X0011X` • yellow (3, currently not vulnerable): `00X0001X` • blue (4, unknown target): `00X00001`
IP Protocol	uint8	Identifier of the IP protocol associated with the event, if applicable.
Network Protocol	uint16	Network protocol associated with the event, if applicable.
Source IP Address	uint8[4]	This field is reserved but no longer populated. The Source IPv4 address is stored in the Source IPv6 Address field. See IP Addresses, page 1-5 for more information.
Source Host Type	uint8	Source host's type: • `0` - Host • `1` - Router • `2` - Bridge

Table 3-24 Correlation Event 5.1+ Data Fields (continued)

Field	Data Type	Description
Source VLAN ID	uint16	Source host's VLAN identification number, if applicable.
Source OS Fingerprint UUID	uint8[16]	A fingerprint ID number that acts a unique identifier for the source host's operating system. See Server Record, page 4-14 for information about obtaining the values that map to the fingerprint IDs.
Source Criticality	uint16	User-defined criticality value for the source host: • 0 - None • 1 - Low • 2 - Medium • 3 - High
Source User ID	uint32	Identification number for the user logged into the source host, as identified by the system.
Source Port	uint16	Source port in the event.
Source Server ID	uint32	Identification number for the server running on the source host.
Destination IP Address	uint8[4]	This field is reserved but no longer populated. The Destination IPv4 address is stored in the Destination IPv6 Address field. See IP Addresses, page 1-5 for more information.
Destination Host Type	uint8	Destination host's type: • 0 - Host • 1 - Router • 2 - Bridge
Destination VLAN ID	uint16	Destination host's VLAN identification number, if applicable.
Destination OS Fingerprint UUID	uint8[16]	A fingerprint ID number that acts as a unique identifier for the destination host's operating system. See Server Record, page 4-14 for information about obtaining the values that map to the fingerprint IDs.
Destination Criticality	uint16	User-defined criticality value for the destination host: • 0 - None • 1 - Low • 2 - Medium • 3 - High
Destination User ID	uint32	Identification number for the user logged into the destination host, as identified by the system.
Destination Port	uint16	Destination port in the event.
Destination Service ID	uint32	Identification number for the server running on the source host.

Table 3-24 Correlation Event 5.1+ Data Fields (continued)

Field	Data Type	Description
Blocked	uint8	Value indicating what happened to the packet that triggered the intrusion event. • 0 - Intrusion event not dropped • 1 - Intrusion event was dropped (drop when deployment is inline, switched, or routed) • 2 - The packet that triggered the event would have been dropped, if the intrusion policy had been applied to a device in inline, switched, or routed deployment.
Ingress Interface UUID	uint8[16]	An interface ID that acts as the unique identifier for the ingress interface associated with correlation event.
Egress Interface UUID	uint8[16]	An interface ID that acts as the unique identifier for the egress interface associated with correlation event.
Ingress Zone UUID	uint8[16]	A zone ID that acts as the unique identifier for the ingress security zone associated with correlation event.
Egress Zone UUID	uint8[16]	A zone ID that acts as the unique identifier for the egress security zone associated with correlation event.
Source IPv6 Address	uint8[16]	IP address of the source host in the event, in IPv6 address octets.
Destination IPv6 Address	uint8[16]	IP address of the destination host in the event, in IPv6 address octets.

The following table describes each Event Defined Mask value.

Table 3-25 Event Defined Values

Description	Mask Value
Event Impact Flags	0x00000001
IP Protocol	0x00000002
Network Protocol	0x00000004
Source IP	0x00000008
Source Host Type	0x00000010
Source VLAN ID	0x00000020
Source Fingerprint ID	0x00000040
Source Criticality	0x00000080
Source Port	0x00000100
Source Server	0x00000200
Destination IP	0x00000400
Destination Host Type	0x00000800
Destination VLAN ID	0x00001000
Destination Fingerprint ID	0x00002000

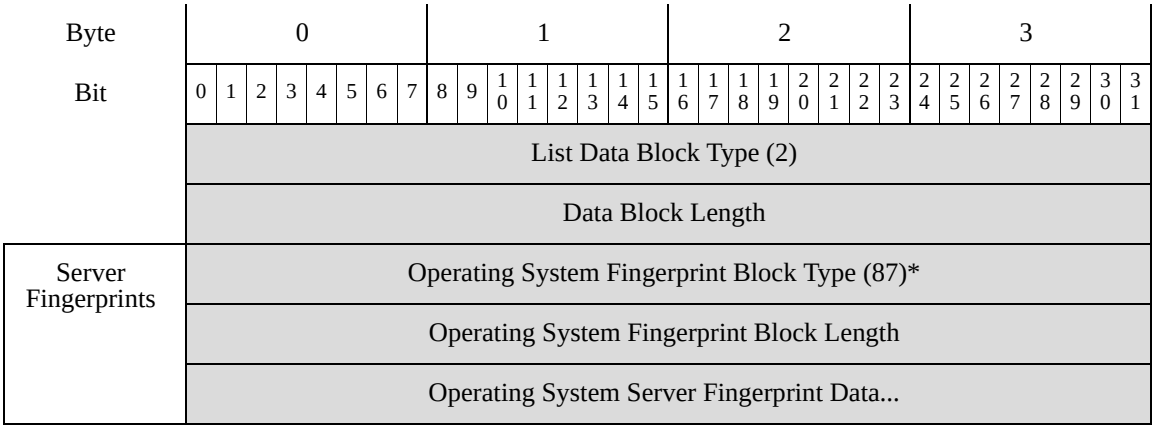
Table 3-25 Event Defined Values (continued)

Description	Mask Value
Destination Criticality	0x00004000
Destination Port	0x00008000
Destination Server	0x00010000
Source User	0x00020000
Destination User	0x00040000

Understanding Series 2 Data Blocks

Beginning in version 4.10.0, the eStreamer service uses a second series of data blocks to package certain records such as intrusion event extra data. See Table 3-26 on page 3-45 for a list of all block types in the series. Series 2 blocks, like series 1 blocks, support variable-length fields and hierarchies of nested blocks. The series 2 block types include primitive blocks that provide the same mechanism for encapsulating nested inner blocks as the series 1 primitive block types. However, series 2 blocks and series 1 blocks have separate numbering systems.

The following example shows the how primitive blocks are used. The list data block (series 2 block type 31) defines an array of operating system fingerprints (each of which is a type 87 block itself with variable length). The overall type 31 data block length is self-describing via the Data Block Length field, which contains the length of the data portion of the message, excluding the 8 bytes in the block type and block length fields.



In the following table, the Data Block Status field indicates whether the block is current (the latest version) or legacy (used in an older version and can still be requested through eStreamer).

Table 3-26 Series 2 Block Types

Type	Content	Data Block Status	Description
0	String	Current	Encapsulates variable string data. See String Data Block, page 3-48 for more information.
1	BLOB	Current	Encapsulates binary data and is used specifically for banners. See BLOB Data Block, page 3-48 for more information.
2	List	Current	Encapsulates a list of other data blocks. See List Data Block, page 3-49 for more information.
3	Generic List	Current	Encapsulates a list of other data blocks. For deserialization, it is the equivalent of the List data block. See Generic List Data Block, page 3-50 for more information.
4	Event Extra Data	Current	Contains intrusion event extra data. See Intrusion Event Extra Data Record, page 3-21 for more information.
5	Extra Data Type	Current	Contains extra data metadata. See Intrusion Event Extra Data Metadata, page 3-23 for more information.
14	UUID String Mapping	Current	Block used by various metadata messages to map UUID values to descriptive strings. See UUID String Mapping Data Block, page 3-51.
15	Access Control Policy Rule ID Metadata	Current	Contains metadata for access control rules. See Access Control Policy Rule ID Metadata Block, page 3-52.
16	Malware Event	Legacy	Contains information on malware events, such as the malware detected or quarantined within a Collective Security Intelligence Cloud, the detection method, and hosts and users affected by the malware. See Malware Event Data Block 5.1, page B-32. Deprecated by block 24, Malware Event Data Block 5.3.1+, page 3-64.
19	ICMP Type Data Block	Current	Contains metadata describing ICMP types. See ICMP Type Data Block, page 3-53.
20	ICMP Code Data Block	Current	Contains metadata describing ICMP codes. See ICMP Code Data Block, page 3-54.
21	Access Control Policy Rule Reason Data Block	Current	Contains information explaining access control policy rule reasons. See Access Control Policy Rule Reason Data Block, page 3-55.
22	IP Reputation Category Data Block	Current	Contains information on IP reputation categories explaining why an IP address was blocked. See IP Reputation Category Data Block, page 3-56.
23	File Event	Legacy	Contains information on file events, such as the source, SHA hash, and the disposition of the file. See File Event for 5.1.1.x, page B-109. It is superseded by block 32, Access Control Policy Rule ID Metadata Block, page 3-52.

Table 3-26 Series 2 Block Types (continued)

Type	Content	Data Block Status	Description
24	Malware Event	Legacy	Contains information on malware events, such as the malware detected or quarantined within a Collective Security Intelligence Cloud, the detection method, and hosts and users affected by the malware. See Malware Event Data Block 5.1.1.x, page B-36. Deprecates block 16, Malware Event Data Block 5.1, page B-32. Deprecated by block 33, Malware Event Data Block 5.3.1+, page 3-64.
25	Intrusion Event	Legacy	Contains information on intrusion events, including information to match intrusion events with connection and malware events. See Intrusion Event Record 5.1.1.x, page B-24. Deprecated by block 34, Intrusion Event Record 5.2.x, page B-11.
26	File Event SHA Hash	Legacy	Contains the SHA hash and name of files that have been identified as containing malware. See File Event SHA Hash for 5.1.1-5.2.x, page B-122. Deprecated by block 40, File Event SHA Hash for 5.3+, page 3-71.
27	Rule Documentation Data Block	Current	Contains information about rules used to generate events. See Rule Documentation Data Block for 5.2+, page 3-73 for more information.
28	Geolocation Data Block	Current	Contains country codes and associated country name. See Geolocation Data Block for 5.2+, page 3-76.
32	File Event	Legacy	Contains information on file events, such as the source, SHA hash, and the disposition of the file. See File Event for 5.2.x, page B-112. It deprecates File Event for 5.1.1.x, page B-109. Deprecated by block 38, File Event for 5.3, page B-116.
33	Malware Event	Current	Contains information on malware events, such as the malware detected or quarantined within a Collective Security Intelligence Cloud, the detection method, and hosts and users affected by the malware. See Malware Event Data Block 5.2.x, page B-42. Deprecates block 24, Malware Event Data Block 5.1.1.x, page B-36. Deprecated by block 35, Malware Event Data Block 5.3, page B-48.
34	Intrusion Event	Legacy	Contains information on intrusion events, including information to match intrusion events with connection and malware events. See Intrusion Event Record 5.2.x, page B-11. Deprecates block 25. Deprecated by block 41, Intrusion Event Record 5.3, page B-17.
35	Malware Event	Legacy	Contains information on malware events, including IOC information. See Malware Event Data Block 5.3, page B-48. Deprecates block 33, Malware Event Data Block 5.2.x, page B-42. Deprecated by block 44, Malware Event Data Block 5.3, page B-48.

Table 3-26 Series 2 Block Types (continued)

Type	Content	Data Block Status	Description
38	File Event	Legacy	Contains information on file events, such as the source, SHA hash, and the disposition of the file. See File Event for 5.3, page B-116. It deprecates block 32. Deprecated by block 43, File Event for 5.3.1+, page 3-57.
39	IOC Name Data Block	Current	Contains information about IOCs. See IOC Name Data Block for 5.3+, page 4-27
40	File Event SHA Hash	Current	Contains the SHA hash and name of files that have been identified as containing malware. See File Event SHA Hash for 5.3+, page 3-71. Deprecates block 26, File Event SHA Hash for 5.1.1-5.2.x, page B-122.
41	Intrusion Event	Legacy	Contains information on intrusion events, including information to match intrusion events with IOCs. See Intrusion Event Record 5.3, page B-17. Deprecates block 34. Deprecated by block 42, Intrusion Event Record 5.3.1+, page 3-6.
42	Intrusion Event	Current	Contains information on intrusion events, including information to match intrusion events with IOCs. See Intrusion Event Record 5.3.1+, page 3-6. Deprecates block 41, Intrusion Event Record 5.3, page B-17.
43	File Event	Current	Contains information on file events, such as the source, SHA hash, and the disposition of the file. See File Event for 5.3.1+, page 3-57. Deprecates block 38, File Event for 5.3, page B-116.
44	Malware Event	Current	Contains information on malware events, including IOC information. See Malware Event Data Block 5.3.1+, page 3-64. Deprecates block 35, Malware Event Data Block 5.3, page B-48.

Series 2 Primitive Data Blocks

Both series 2 and series 1 blocks include a set of primitives that are used to encapsulate lists of variable-length blocks as well as variable-length strings and BLOBs within messages. These primitive blocks have the standard eStreamer block header discussed above in Data Block Header, page 2-24, but they appear only within other data blocks. Any number can be included in a given block type. For details on the structure of these blocks, see the following:

- String Data Block, page 3-48
- BLOB Data Block, page 3-48
- List Data Block, page 3-49
- Generic List Data Block, page 3-50

String Data Block

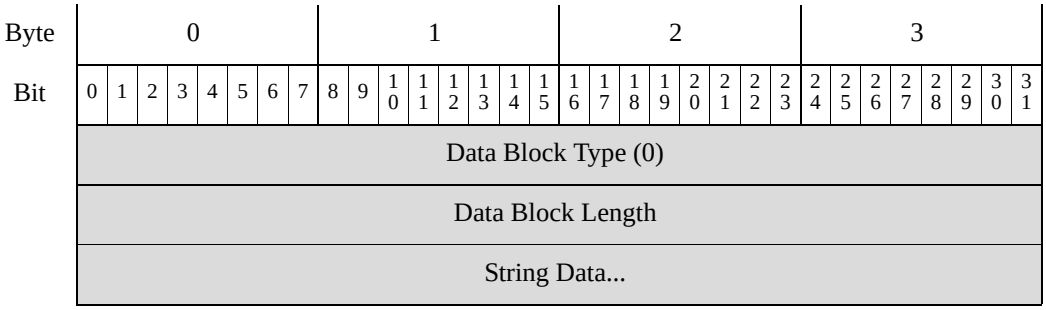
The eStreamer service uses the String data block to send string data in messages. These blocks commonly appear within other data blocks to identify, for example, operating system or server names.

Empty String data blocks (containing no data, only the header fields) have a block length of 8. eStreamer uses an empty String data block when it has no content for a string value, as might happen, for example, in the OS vendor string field in an Operating System data block when the vendor of the operating system is unknown.

The String data block has a block type of 0 in the series 2 group of blocks.

Note Strings returned in this data block are not always null-terminated (that is, the string characters are not always followed by a 0).

The following diagram shows the format of the String data block:



The following table describes the fields of the String data block.

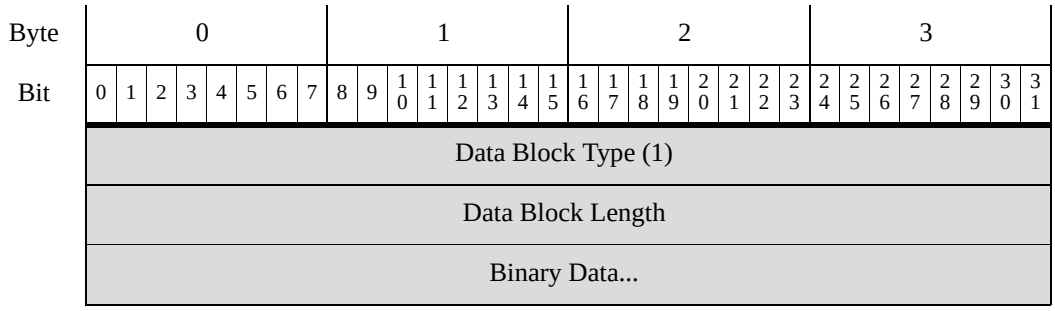
Table 3-27 String Block Fields

Field	Data Type	Description
Data Block Type	uint32	Initiates a String data block. This value is always `0`.
Data Block Length	uint32	Combined length in bytes of the string data block header and string data.
String Data	string	Contains the string data and may contain a terminating character (null byte) at the end of the string.

BLOB Data Block

The eStreamer service uses the BLOB data block to convey binary data. For example, host discovery records use the BLOB block to hold captured server banners. The BLOB data block has a block type of 1 in the series 2 group of blocks.

The following diagram shows the format of the BLOB data block:



The following table describes the fields of the BLOB data block.

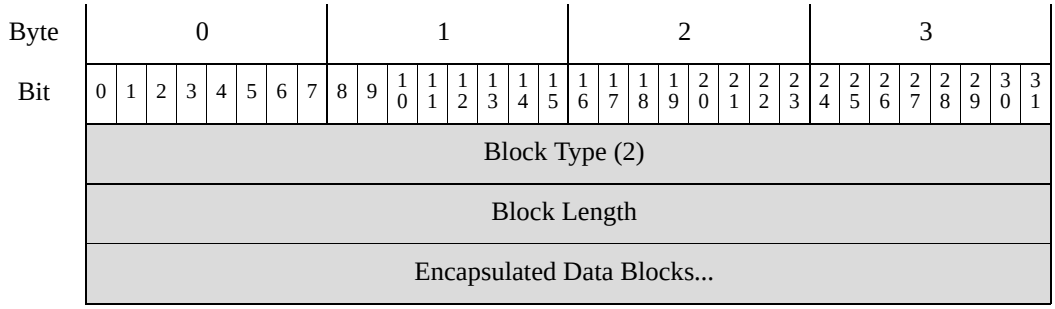
Table 3-28 BLOB Data Block Fields

Field	Data Type	Description
Data Block Type	uint32	Initiates a BLOB data block. This value is always `1`.
Data Block Length	uint32	Number of bytes in the BLOB data block, including eight bytes for the BLOB block type and length fields, plus the length of the binary data that follows.
Binary Data	variable	Contains binary data such as a server banner.

List Data Block

The eStreamer service uses the List data block to encapsulate a list of data blocks. For example, eStreamer can use the List data block to send a list of TCP servers, each of which is itself a data block. The List data block has a block type of 2 in the series 2 group of blocks.

The following diagram shows the basic format of a List data block:



The following table describes the fields of the List data block.

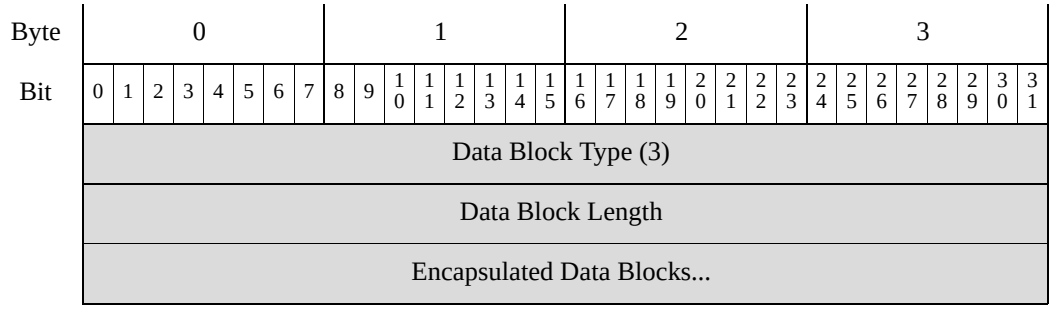
Table 3-29 List Data Fields

Field	Data Type	Description
Block Type	uint32	Initiates a List data block. This value is always 2.
Block Length	uint32	Number of bytes in the List block and encapsulated data. For example, if there were three Sub-Server data blocks included in the list, the value here would include the total number of bytes in the Sub-Server blocks, plus eight bytes for the List block header.
Encapsulated Data Blocks	variable	Encapsulated data blocks up to the maximum number of bytes in the list block length.

Generic List Data Block

The eStreamer service uses the Generic List data block to encapsulate a list of data blocks. For example, the Host Profile data block contains information about multiple client applications and uses the Generic List block to embed a list of Client Application data blocks in the message. The Generic List data block has a block type of 3 in the series 2 group of blocks.

The following diagram shows the basic structure of a Generic List data block:



The following table describes the fields of the Generic List data block.

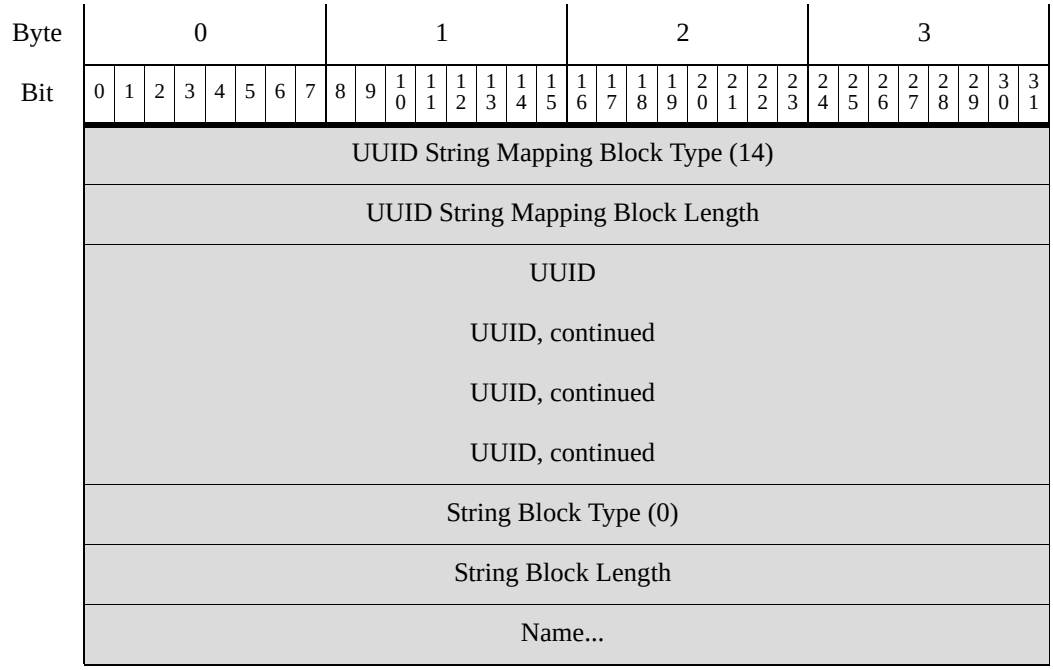
Table 3-30 Generic List Data Block Fields

Field	Number of Bytes	Description
Data Block Type	uint32	Initiates a Generic List data block. This value is always 3.
Data Block Length	uint32	Number of bytes in the Generic List block and encapsulated data blocks. This number includes the eight bytes of the generic list block header fields, plus the total number of bytes in all of the encapsulated data blocks.
Encapsulated Data Blocks	variable	Encapsulated data blocks up to the maximum number of bytes in the Generic List block length.

UUID String Mapping Data Block

The eStreamer service uses the UUID String Mapping data block in various metadata messages to map UUID values to descriptive strings. The UUID String Mapping data block has a block type of 14 in series 2.

The following diagram shows the structure of the UUID String Mapping data block.



The following table describes the fields in the UUID String Mapping data block.

Table 3-31 UUID String Mapping Data Block Fields

Field	Data Type	Description
UUID String Mapping Block Type	uint32	Initiates a UUID String Mapping block. This value is always `14`.
UUID String Mapping Block Length	uint32	Total number of bytes in the UUID String Mapping block, including eight bytes for the UUID String Mapping block type and length fields, plus the number of bytes of data that follows.
UUID	uint8[16]	The unique identifier for the event or other object the UUID identifies.
String Block Type	uint32	Initiates a String data block containing the descriptive name associated with the UUID. This value is always `0`.
String Block Length	uint32	The number of bytes included in the name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Name field.
Name	string	The descriptive name.

Access Control Policy Rule ID Metadata Block

The eStreamer service uses the Access Control Policy Rule ID metadata block to contain information about access control policy rule IDs. This data block has a block type of 15 in series 2.

The following diagram shows the structure of the Access Control Policy Rule ID metadata block.

	Byte	0								1								2								3							
	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	Access Control Policy Rule ID Metadata Block Type (15)																																
	Access Control Policy Rule ID Metadata Block Length																																
	Revision Revision, continued Revision, continued Revision, continued																																
	Rule ID																																
Name	String Block Type (0)																																
	String Block Length																																
	Name...																																

The following table describes the fields in the Access Control Policy Rule ID Metadata block.

Table 3-32 *Access Control Policy Rule ID Metadat**a Block Fields***

Field	Data Type	Description
Access Control Policy Rule ID Metadata Block Type	uint32	Initiates a Access Control Policy Rule ID Metadata block. This value is always `15`.
Access Control Policy Rule ID Metadata Block Length	uint32	Total number of bytes in the Access Control Policy Rule ID block, including eight bytes for the Access Control Policy Rule ID metadata block type and length fields, plus the number of bytes of data that follows.
Revision	uint8[16]	Revision number of the rule associated with the triggered correlation event.
Rule ID	uint32	Internal identifier for the rule that triggered the event.
String Block Type	uint32	Initiates a String data block containing the descriptive name associated with the access control policy rule. This value is always `0`.

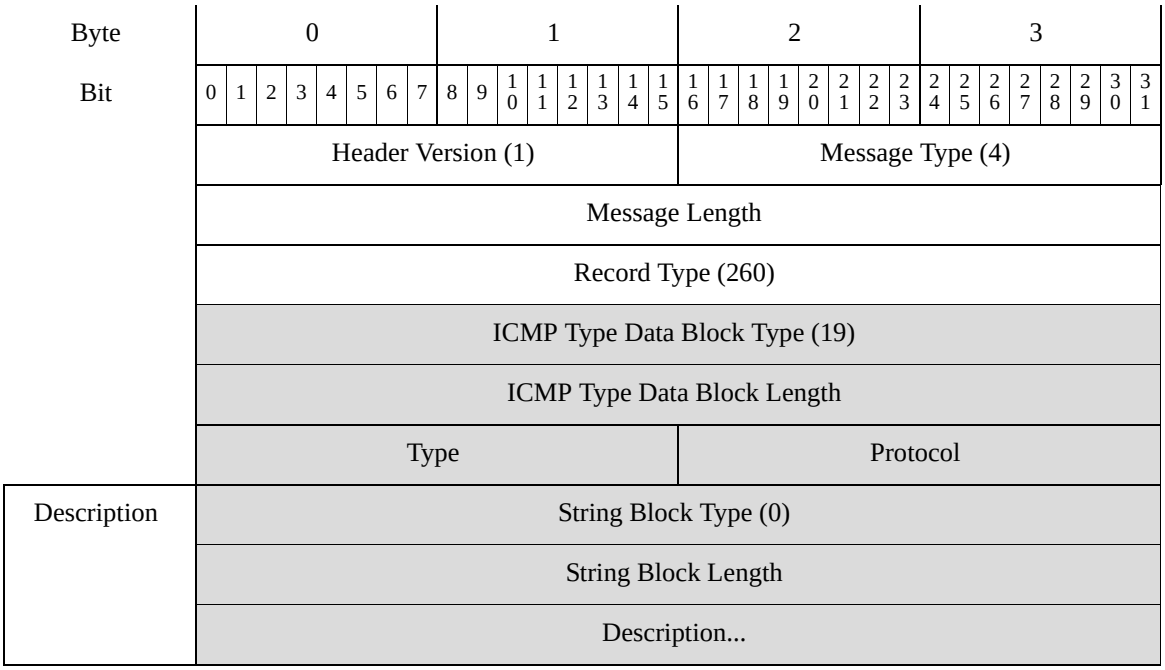
Table 3-32 Access Control Policy Rule ID Metadata Block Fields (continued)

Field	Data Type	Description
String Block Length	uint32	The number of bytes included in the name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Name field.
Name	string	The descriptive name of the access control policy rule.

ICMP Type Data Block

The eStreamer service uses the ICMP Type data block to contain information about ICMP Types. This data block has a record type of 260, and a block type of 19 in series 2.

The following diagram shows the structure of the ICMP Type data block.



The following table describes the fields in the ICMP Type data block.

Table 3-33 ICMP Type Data Block Fields

Field	Data Type	Description
ICMP Type Data Block Type	uint32	Initiates an ICMP Type data block. This value is always `19`.
ICMP Type Data Block Length	uint32	Total number of bytes in the ICMP Type data block, including eight bytes for the ICMP Type data block type and length fields, plus the number of bytes of data that follows.
Type	uint16	The ICMP type of the event.

Table 3-33 ICMP Type Data Block Fields (continued)

Field	Data Type	Description
Protocol	uint16	IANA-specified protocol number. For example: • 0 - IP • 1 - ICMP • 6 - TCP • 17 - UDP
String Block Type	uint32	Initiates a String data block containing the description of the ICMP type. This value is always 0.
String Block Length	uint32	The number of bytes included in the name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Description field.
Description	string	Description of the ICMP type for the event.

ICMP Code Data Block

The eStreamer service uses the ICMP Code data block to contain information about access control policy rule IDs. This data block has a record type of 270, and block type of 20 in series 2.

The following diagram shows the structure of the Access Control Policy Rule ID metadata block.

Byte	0								1								2								3							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	Header Version (1)																Message Type (4)															
	Message Length																															
	Record Type (270)																															
	ICMP Code Data Block Type (20)																															
	ICMP Code Data Block Length																															
	Code																Type															
Description	Protocol																String Block Type (0)															
	String Block Type (0), continued																String Block Length															
	String Block Length, continued																Description...															

The following table describes the fields in the ICMP Code data block.

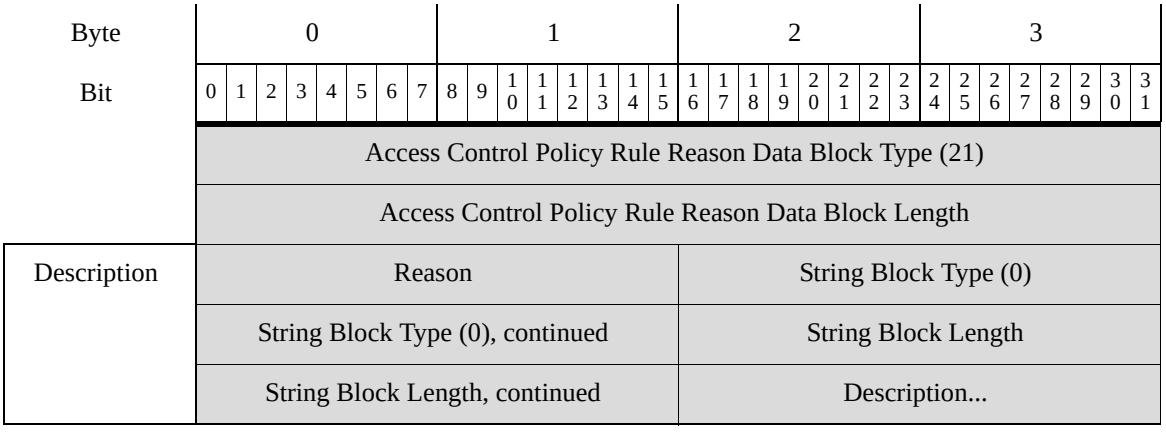
Table 3-34 ICMP Code Data Block Fields

Field	Data Type	Description
ICMP Code Data Block Type	uint32	Initiates a ICMP Code data block. This value is always `20`.
ICMP Code Data Block Length	uint32	Total number of bytes in the ICMP Code data block, including eight bytes for the ICMP Code data block type and length fields, plus the number of bytes of data that follows.
Code	uint16	The ICMP code of the event.
Type	uint16	The ICMP type of the event.
Protocol	uint16	IANA-specified protocol number. For example: • `0` - IP • `1` - ICMP • `6` - TCP • `17` - UDP
String Block Type	uint32	Initiates a String data block containing the description of the ICMP code. This value is always `0`.
String Block Length	uint32	The number of bytes included in the name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Description field.
Description	string	Description of the ICMP code for the event.

Access Control Policy Rule Reason Data Block

The eStreamer service uses the Access Control Rule Policy Rule Reason Data block to contain information about access control policy rule IDs. This data block has a block type of 21 in series 2.

The following diagram shows the structure of the Access Control Policy Rule ID metadata block.



The following table describes the fields in the Access Control Policy Rule ID metadata block.

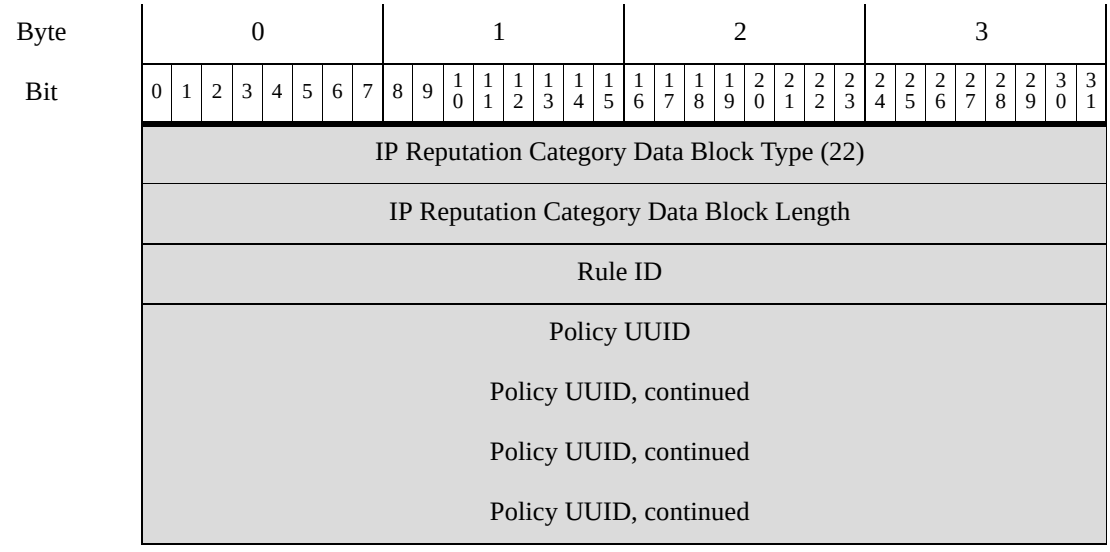
Table 3-35 Access Control Policy Rule Reason Data Block Fields

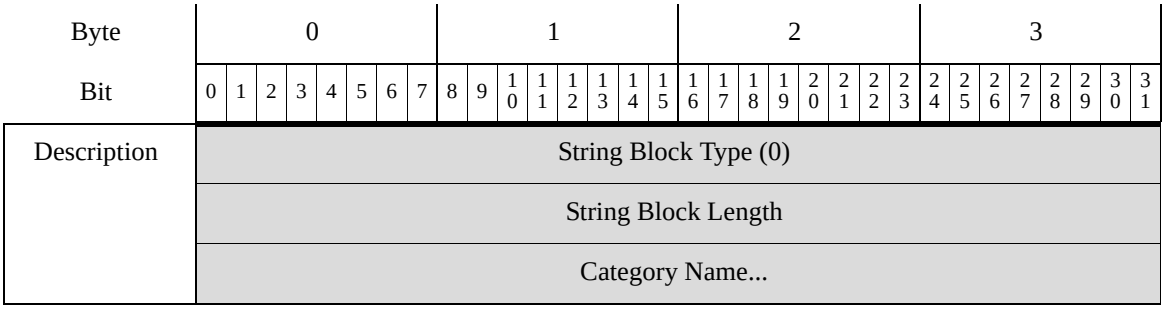
Field	Data Type	Description
Access Control Policy Rule Reason Data Block Type	uint32	Initiates an Access Control Policy Rule Reason data block. This value is always `21`.
Access Control Policy Rule Reason Data Block Length	uint32	Total number of bytes in the Access Control Policy Rule Reason data block, including eight bytes for the Access Control Policy Rule Reason data block type and length fields, plus the number of bytes of data that follows.
Reason	uint16	The number of the reason for the rule that triggered the event.
String Block Type	uint32	Initiates a String data block containing the description of the access control policy rule reason. This value is always `0`.
String Block Length	uint32	The number of bytes included in the name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Description field.
Description	string	Description of the reason for the rule.

IP Reputation Category Data Block

The eStreamer service uses the IP Reputation Category Data block to contain information about rule reputation categories. This data block has a block type of 22 in series 2.

The following diagram shows the structure of the IP Reputation Category data block.





The following table describes the fields in the IP Reputation Category Data Block.

Table 3-36 IP Reputation Category Data Block Fields

Field	Data Type	Description
IP Reputation Category Data Block Type	uint32	Initiates a IP Reputation Category data block. This value is always `22`.
IP Reputation Category Data Block Length	uint32	Total number of bytes in the IP Reputation Category data block, including eight bytes for the IP Reputation Category data block type and length fields, plus the number of bytes of data that follows.
Rule ID	uint32	Internal identifier for the rule that triggered the event.
Policy UUID	uint8[16]	UUID of the policy that triggered the event.
String Block Type	uint32	Initiates a String data block containing the description of the IP Reputation Category. This value is always `0`.
String Block Length	uint32	The number of bytes included in the Category Name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Category Name field.
Category Name	string	Name of the category for the rule.

File Event for 5.3.1+

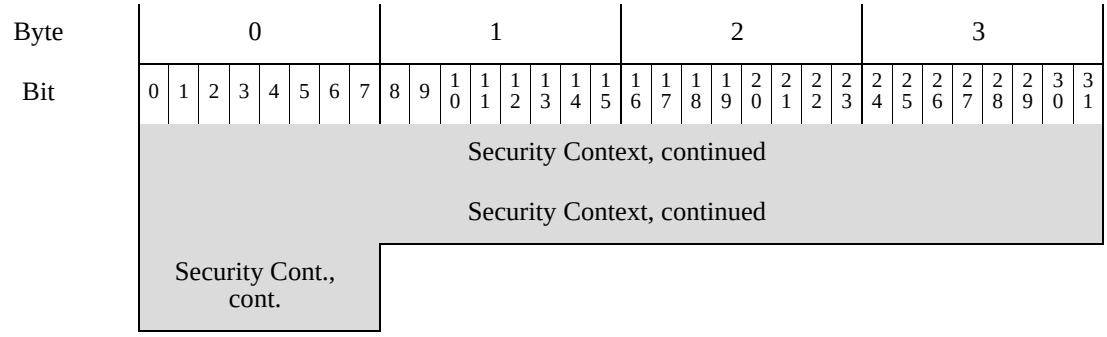
The file event contains information on files that are sent over the network. This includes the connection information, whether the file is malware, and specific information to identify the file. The file event has a block type of 43 in the series 2 group of blocks. It supersedes block type 38. A security context field has been added.

You request file event records by setting the file event flag—bit 30 in the Request Flags field—in the request message with an event version of 4 and an event code of 111. See Request Flags, page 2-11. If you enable bit 23, an extended event header is included in the record.

The following graphic shows the structure of the File Event data block.

Byte	0								1								2								3							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
File Event Block Type (43)																																
File Event Block Length																																
Device ID																																
Connection Instance																	Connection Counter															
Connection Timestamp																																
File Event Timestamp																																
Source IP Address Source IP Address, continued Source IP Address, continued Source IP Address, continued																																
Destination IP Address Destination IP Address, continued Destination IP Address, continued Destination IP Address, continued																																
Disposition									SPERO Disposition								File Storage Status								File Analysis Status							
Archive File Status									Threat Score								Action								SHA Hash							
SHA Hash, continued SHA Hash, continued SHA Hash, continued SHA Hash, continued SHA Hash, continued SHA Hash, continued SHA Hash, continued																																
SHA Hash, continued																									File Type ID							

Byte	0								1								2								3							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
File Name	File Type ID, cont.																								String Block Type (0)							
	String Block Type (0), cont.																								String Block Length							
	String Block Length, cont.																								File Name...							
	File Size File Size, continued																															
	Direction								Application ID																							
	App ID, cont.								User ID																							
URI	User ID, cont.								String Block Type (0)																							
	String Block Type (0), cont.								String Block Length																							
	String Block Length, cont.								URI...																							
Signature	String Block Type (0)																															
	String Block Length																															
	Signature...																															
	Source Port																Destination Port															
	Protocol								Access Control Policy UUID																							
	Access Control Policy UUID, continued Access Control Policy UUID, continued Access Control Policy UUID, continued																															
	AC Pol UUID, cont.								Source Country																Dst. Country							
	Dst. Country, cont.								Web Application ID																							
	Web App. ID, cont.								Client Application ID																							
	Client App. ID, cont.								Security Context																							
	Security Context, continued																															



The following table describes the fields in the file event data block.

Table 3-37 File Event Data Block for 5.3.1+ Fields

Field	Data Type	Description
File Event Block Type	uint32	Initiates whether file event data block. This value is always `43`.
File Event Block Length	uint32	Total number of bytes in the file event block, including eight bytes for the file event block type and length fields, plus the number of bytes of data that follows.
Device ID	uint32	ID for the device that generated the event.
Connection Instance	uint16	Snort instance on the device that generated the event. Used to link the event with a connection or intrusion event.
Connection Counter	uint16	Value used to distinguish between connection events that happen during the same second.
Connection Timestamp	uint32	UNIX timestamp (seconds since 01/01/1970) of the associated connection event.
File Event Timestamp	uint32	UNIX timestamp (seconds since 01/01/1970) of when the file type is identified and the file event generated.
Source IP Address	uint8[16]	IPv4 or IPv6 address for the source of the connection.
Destination IP Address	uint8[16]	IPv4 or IPv6 address for the destination of the connection.
Disposition	uint8	The malware status of the file. Possible values include: • `1` - CLEAN The file is clean and does not contain malware. • `2` - UNKNOWN It is unknown whether the file contains malware. • `3` - MALWARE The file contains malware. • `4` - UNAVAILABLE The software was unable to send a request to the Cisco cloud for a disposition, or the Cisco cloud services did not respond to the request. • `5` - CUSTOM SIGNATURE The file matches a user-defined hash, and is treated in a fashion designated by the user.

Table 3-37 File Event Data Block for 5.3.1+ Fields (continued)

Field	Data Type	Description
SPERO Disposition	uint8	Indicates whether the SPERO signature was used in file analysis. If the value is 1, 2, or 3, SPERO analysis was used. If there is any other value SPERO analysis was not used.
File Storage Status	uint8	The storage status of the file. Possible values are: • 1 - File Stored • 2 - File Stored • 3 - Unable to Store File • 4 - Unable to Store File • 5 - Unable to Store File • 6 - Unable to Store File • 7 - Unable to Store File • 8 - File Size is Too Large • 9 - File Size is Too Small • 10 - Unable to Store File • 11 - File Not Stored, Disposition Unavailable

Table 3-37 File Event Data Block for 5.3.1+ Fields (continued)

Field	Data Type	Description
File Analysis Status	uint8	Indicates whether the file was sent for dynamic analysis. Possible values are: • 1 - Sent for Analysis • 2 - Sent for Analysis • 4 - Sent for Analysis • 5 - Failed to Send • 6 - Failed to Send • 7 - Failed to Send • 8 - Failed to Send • 9 - File Size is Too Small • 10 - File Size is Too Large • 11 - Sent for Analysis • 12 - Analysis Complete • 13 - Failure (Network Issue) • 14 - Failure (Rate Limit) • 15 - Failure (File Too Large) • 16 - Failure (File Read Error) • 17 - Failure (Internal Library Error) • 19 - File Not Sent, Disposition Unavailable • 20 - Failure (Cannot Run File) • 21 - Failure (Analysis Timeout) • 22 - Sent for Analysis • 23 - File Not Supported
Archive File Status	uint8	This is always 0.
Threat Score	uint8	A numeric value from 0 to 100 based on the potentially malicious behaviors observed during dynamic analysis.
Action	uint8	The action taken on the file based on the file type. Can have the following values: • 1 - Detect • 2 - Block • 3 - Malware Cloud Lookup • 4 - Malware Block • 5 - Malware Whitelist • 6 - Cloud Lookup Timeout • 7 - Custom Detection • 8 - Custom Detection Block

Table 3-37 File Event Data Block for 5.3.1+ Fields (continued)

Field	Data Type	Description
SHA Hash	uint8[32]	SHA-256 hash of the file, in binary format.
File Type ID	uint32	ID number that maps to the file type. The meaning of this field is transmitted in the metadata with this event. See FireAMP File Type Metadata, page 3-35 for more information.
File Name	string	Name of the file.
File Size	uint64	Size of the file in bytes.
Direction	uint8	Value that indicates whether the file was uploaded or downloaded. Can have the following values: • `1` - Download • `2` - Upload Currently the value depends on the protocol (for example, if the connection is HTTP it is a download).
Application ID	uint32	ID number that maps to the application using the file transfer.
User ID	uint32	ID number for the user logged into the destination host, as identified by the system.
URI	string	Uniform Resource Identifier (URI) of the connection.
Signature	string	SHA-256 hash of the file, in string format.
Source Port	uint16	Port number for the source of the connection.
Destination Port	uint16	Port number for the destination of the connection.
Protocol	uint8	IANA protocol number specified by the user. For example: • `1` - ICMP • `4` - IP • `6` - TCP • `17` - UDP This is currently only TCP.
Access Control Policy UUID	uint8[16]	Unique identifier for the access control policy that triggered the event.
Source Country	uint16	Code for the country of the source host.
Destination Country	uint16	Code for the country of the destination host.
Web Application ID	uint32	The internal identification number for the web application, if applicable.
Client Application ID	uint32	The internal identification number for the client application, if applicable.
Security Context	uint8(16)	ID number for the security context (virtual firewall) that the traffic passed through. Note that the system only populates this field for ASA FirePOWER devices in multi-context mode.

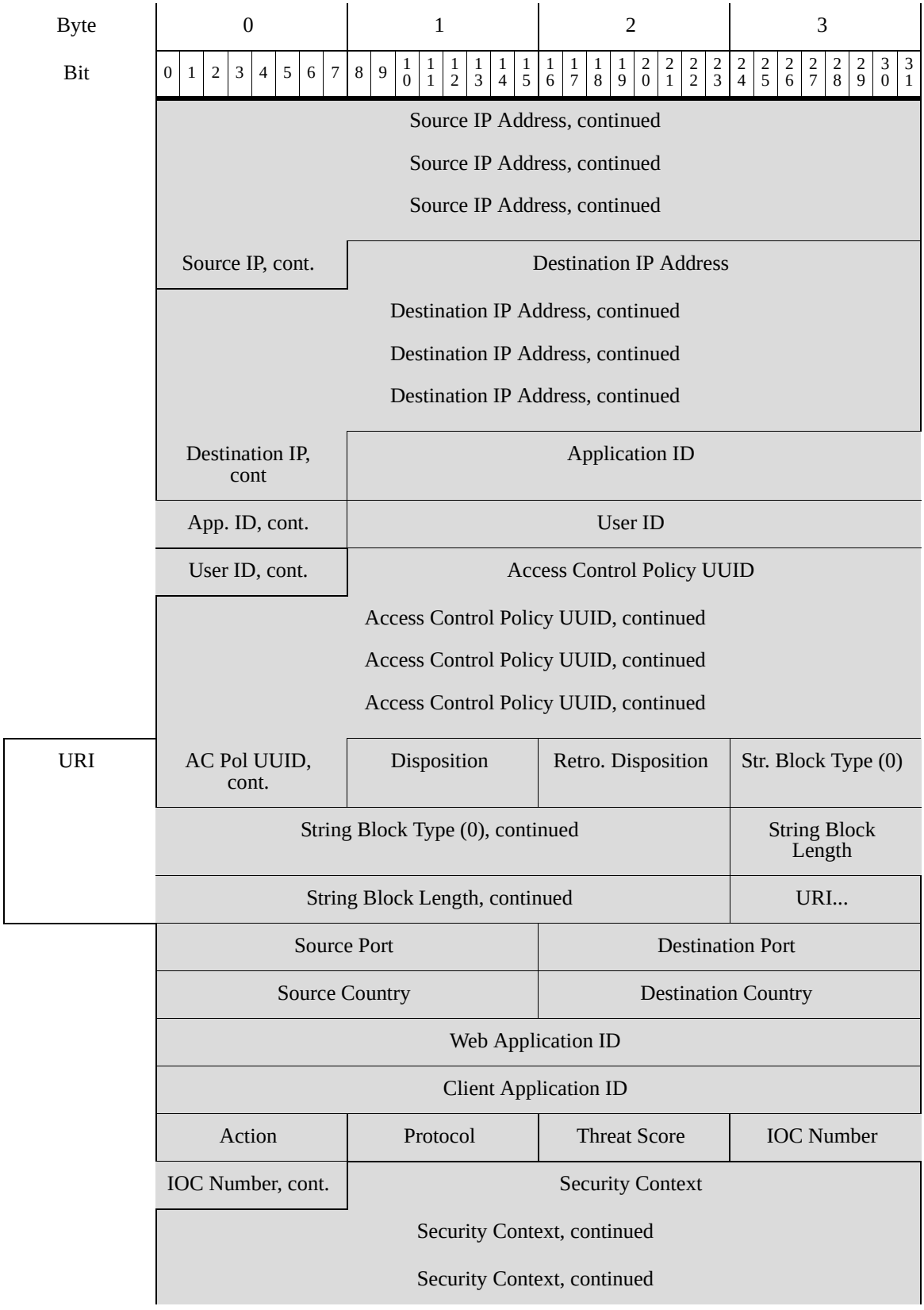
Malware Event Data Block 5.3.1+

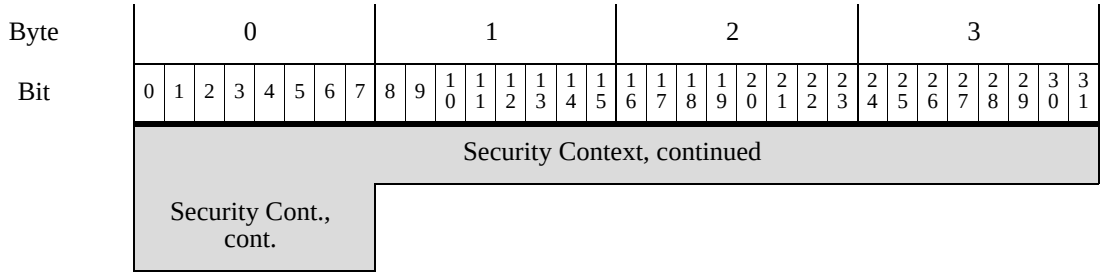
The eStreamer service uses the malware event data block to store information on malware events. These events contain information on malware detected or quarantined within a cloud, the detection method, and hosts and users affected by the malware. The malware event data block has a block type of 44 in the series 2 group of blocks. It supersedes block 35. You request the event as part of the malware event record by setting the malware event flag—bit 30 in the request flags field—in the request message with an event version of 5 and an event code of 101.

The following graphic shows the structure of the malware event data block:

Byte	0								1								2								3							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	Malware Event Block Type (44)																															
	Malware Event Block Length																															
	Agent UUID Agent UUID, continued Agent UUID, continued Agent UUID, continued																															
	Cloud UUID Cloud UUID, continued Cloud UUID, continued Cloud UUID, continued																															
	Malware Event Timestamp																															
	Event Type ID																															
	Event Subtype ID																															
Detection Name	Detector ID								String Block Type (0)																							
	String Block Type (0), cont.								String Block Length																							
	String Block Length, cont.								Detection Name...																							
User	String Block Type (0)																															
	String Block Length																															
	User...																															


Byte
0
1
2
3
Bit
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
File Name
String Block Type (0)
String Block Length
File Name...
File Path
String Block Type (0)
String Block Length
File Path...
File SHA Hash
String Block Type (0)
String Block Length
File SHA Hash...
File Size
File Type
File Timestamp
Parent File Name
String Block Type (0)
String Block Length
Parent File Name...
Parent File SHA Hash
String Block Type (0)
String Block Length
Parent File SHA Hash...
Event Description
String Block Type (0)
String Block Length
Event Description...
Device ID
Connection Instance
Connection Counter
Connection Event Timestamp
Direction
Source IP Address


Byte
0
1
2
3
Bit
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Source IP Address, continued
Source IP Address, continued
Source IP Address, continued
Source IP, cont.
Destination IP Address
Destination IP Address, continued
Destination IP Address, continued
Destination IP Address, continued
Destination IP, cont
Application ID
App. ID, cont.
User ID
User ID, cont.
Access Control Policy UUID
Access Control Policy UUID, continued
Access Control Policy UUID, continued
Access Control Policy UUID, continued
URI
AC Pol UUID, cont.
Disposition
Retro. Disposition
Str. Block Type (0)
String Block Type (0), continued
String Block Length
String Block Length, continued
URI...
Source Port
Destination Port
Source Country
Destination Country
Web Application ID
Client Application ID
Action
Protocol
Threat Score
IOC Number
IOC Number, cont.
Security Context
Security Context, continued
Security Context, continued



The following table describes the fields in the malware event data block.

Table 3-38 Malware Event Data Block for 5.3.1+ Fields

Field	Data Type	Description
Malware Event Block Type	uint32	Initiates a malware event data block. This value is always 44.
Malware Event Block Length	uint32	Total number of bytes in the malware event data block, including eight bytes for the malware event block type and length fields, plus the number of bytes of data that follows.
Agent UUID	uint8[16]	The internal unique ID of the FireAMP agent reporting the malware event.
Cloud UUID	uint8[16]	The internal unique ID of the Collective Security Intelligence Cloud from which the malware event originated.
Malware Event Timestamp	uint32	The malware event generation timestamp.
Event Type ID	uint32	The internal ID of the malware event type.
Event Subtype ID	uint32	The internal ID of the action that led to malware detection.
Detector ID	uint8	The internal ID of the detection technology that detected the malware.
String Block Type	uint32	Initiates a String data block containing the detection name. This value is always 0.
String Block Length	uint32	The number of bytes included in the Detection Name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Detection Name field.
Detection Name	string	The name of the detected or quarantined malware.
String Block Type	uint32	Initiates a String data block containing the username. This value is always 0.
String Block Length	uint32	The number of bytes included in the User String data block, including eight bytes for the block type and header fields plus the number of bytes in the User field.
User	string	The user of the computer where the Cisco Agent is installed and where the malware event occurred. Note that these users are not tied to user discovery.

Table 3-38 Malware Event Data Block for 5.3.1+ Fields (continued)

Field	Data Type	Description
String Block Type	uint32	Initiates a String data block containing the file name. This value is always 0.
String Block Length	uint32	The number of bytes included in the File Name String data block, including eight bytes for the block type and header fields plus the number of bytes in the File Name field.
File Name	string	The name of the detected or quarantined file.
String Block Type	uint32	Initiates a String data block containing the file path. This value is always 0.
String Block Length	uint32	The number of bytes included in the File Path String data block, including eight bytes for the block type and header fields plus the number of bytes in the File Path field.
File Path	string	The file path, not including the file name, of the detected or quarantined file.
String Block Type	uint32	Initiates a String data block containing the file SHA hash. This value is always 0.
String Block Length	uint32	The number of bytes included in the File SHA Hash String data block, including eight bytes for the block type and header fields plus the number of bytes in the File SHA Hash field.
File SHA Hash	string	The rendered string of the SHA-256 hash value of the detected or quarantined file.
File Size	uint32	The size in bytes of the detected or quarantined file.
File Type	uint32	The file type of the detected or quarantined file. The meaning of this field is transmitted in the metadata with this event. See FireAMP File Type Metadata, page 3-35 for more information.
File Timestamp	uint32	UNIX timestamp (seconds since 01/01/1970) of the creation of the detected or quarantined file.
String Block Type	uint32	Initiates a String data block containing the parent file name. This value is always 0.
String Block Length	uint32	The number of bytes included in the Parent File Name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Parent File Name field.
Parent File Name	string	The name of the file accessing the detected or quarantined file when detection occurred.
String Block Type	uint32	Initiates a String data block containing the parent file SHA hash. This value is always 0.
String Block Length	uint32	The number of bytes included in the Parent File SHA Hash String data block, including eight bytes for the block type and header fields plus the number of bytes in the Parent File SHA Hash field.

Table 3-38 Malware Event Data Block for 5.3.1+ Fields (continued)

Field	Data Type	Description
Parent File SHA Hash	string	The SHA-256 hash value of the parent file accessing the detected or quarantined file when detection occurred.
String Block Type	uint32	Initiates a String data block containing the event description. This value is always `0`.
String Block Length	uint32	The number of bytes included in the Event Description String data block, including eight bytes for the block type and header fields plus the number of bytes in the Event Description field.
Event Description	string	The additional event information associated with the event type.
Device ID	uint32	ID for the device that generated the event.
Connection Instance	uint16	Snort instance on the device that generated the event. Used to link the event with a connection or IDS event.
Connection Counter	uint16	Value used to distinguish between connection events that happen during the same second.
Connection Event Timestamp	uint32	Timestamp of the connection event.
Direction	uint8	Indicates whether the file was uploaded or downloaded. Can have the following values: • `1` - Download • `2` - Upload Currently the value depends on the protocol (for example, if the connection is HTTP it is a download).
Source IP Address	uint8[16]	IPv4 or IPv6 address for the source of the connection.
Destination IP Address	uint8[16]	IPv4 or IPv6 address for the destination of the connection.
Application ID	uint32	ID number that maps to the application using the file transfer.
User ID	uint32	Identification number for the user logged into the destination host, as identified by the system.
Access Control Policy UUID	uint8[16]	Identification number that acts as a unique identifier for the access control policy that triggered the event.

Table 3-38 Malware Event Data Block for 5.3.1+ Fields (continued)

Field	Data Type	Description
Disposition	uint8	The malware status of the file. Possible values include: • 1 - CLEAN The file is clean and does not contain malware. • 2 - UNKNOWN It is unknown whether the file contains malware. • 3 - MALWARE The file contains malware. • 4 - UNAVAILABLE The software was unable to send a request to the Cisco cloud for a disposition, or the Cisco cloud services did not respond to the request. • 5 - CUSTOM SIGNATURE The file matches a user-defined hash, and is treated in a fashion designated by the user.
Retrospective Disposition	uint8	Disposition of the file if the disposition is updated. If the disposition is not updated, this field contains the same value as the Disposition field. The possible values are the same as the Disposition field.
String Block Type	uint32	Initiates a String data block containing the URI. This value is always 0.
String Block Length	uint32	The number of bytes included in the URI data block, including eight bytes for the block type and header fields plus the number of bytes in the URI field.
URI	string	URI of the connection.
Source Port	uint16	Port number for the source of the connection.
Destination Port	uint16	Port number for the destination of the connection.
Source Country	uint16	Code for the country of the source host.
Destination Country	uint 16	Code for the country of the destination host.
Web Application ID	uint32	The internal identification number of the detected web application, if applicable.
Client Application ID	uint32	The internal identification number of the detected client application, if applicable.
Action	uint8	The action taken on the file based on the file type. Can have the following values: • 1 - Detect • 2 - Block • 3 - Malware Cloud Lookup • 4 - Malware Block • 5 - Malware Whitelist • 6 - Cloud Lookup Timeout • 7 - Custom Detection • 8 - Custom Detection Block

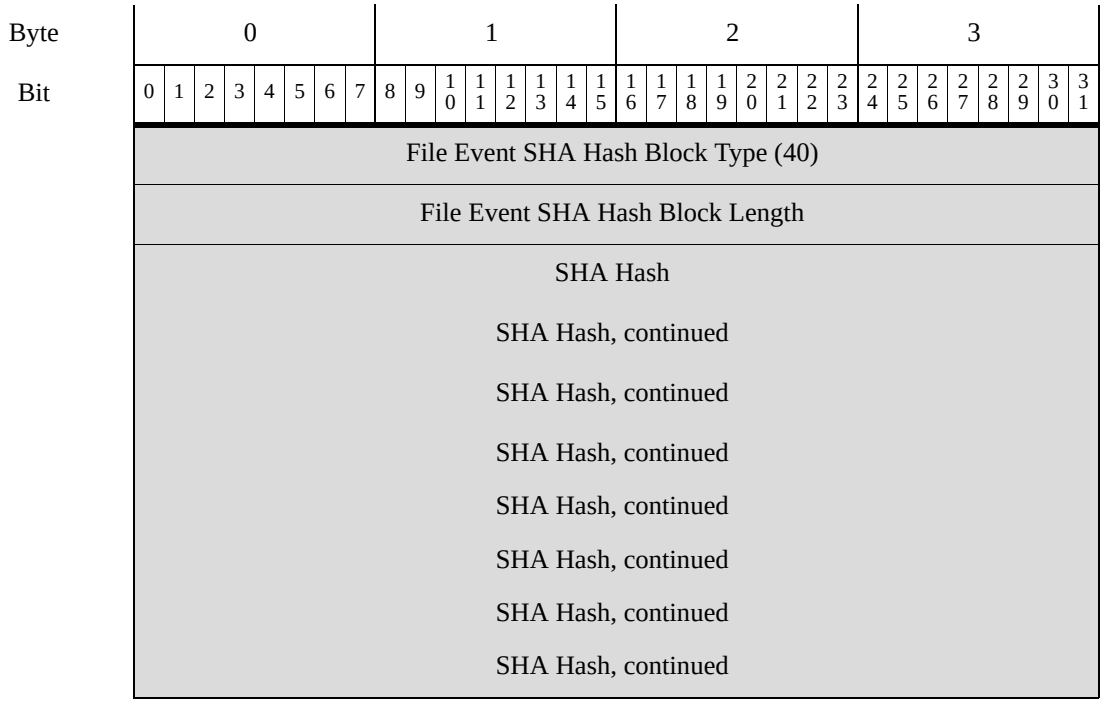
Table 3-38 Malware Event Data Block for 5.3.1+ Fields (continued)

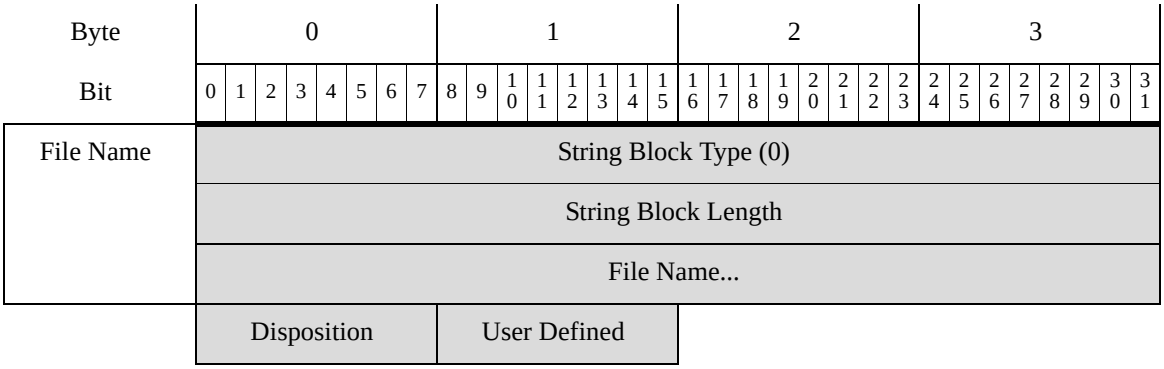
Field	Data Type	Description
Protocol	uint8	IANA protocol number specified by the user. For example: • 1 - ICMP • 4 - IP • 6 - TCP • 17 - UDP This is currently only TCP.
Threat Score	uint8	A numeric value from 0 to 100 based on the potentially malicious behaviors observed during dynamic analysis.
IOC Number	uint16	ID number of the compromise associated with this event.
Security Context	uint8(16)	ID number for the security context (virtual firewall) that the traffic passed through. Note that the system only populates this field for ASA FirePOWER devices in multi-context mode.

File Event SHA Hash for 5.3+

The eStreamer service uses the File Event SHA Hash data block to contain metadata of the mapping of the SHA hash of a file to its filename. The block type is 40 in the series 2 list of data blocks. It can be requested if file log events have been requested in the extended requests—event code 111—and either bit 20 is set or metadata is requested with an event version of 5 and an event code of 21.

The following diagram shows the structure of a file event hash data block:





The following table describes the fields in the file event SHA hash data block.

Table 3-39 File Event SHA Hash Data Block Fields

Field	Data Type	Description
File Event SHA Hash Block Type	uint32	Initiates a File Event SHA Hash block. This value is always `26`.
File Event SHA Hash Block Length	uint32	Total number of bytes in the File Event SHA Hash block, including eight bytes for the File Event SHA Hash block type and length fields, plus the number of bytes of data that follows.
SHA Hash	uint8[32]	The SHA-256 hash of the file in binary format.
String Block Type	uint32	Initiates a String data block containing the descriptive name associated with the file. This value is always `0`.
String Block Length	uint32	The number of bytes included in the name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Name field.
File Name or Disposition	string	The descriptive name or disposition of the file. If the file is clean, this value is `Clean`. If the file's disposition is unknown, the value is `Neutral`. If the file contains malware, the file name is given.
Disposition	uint8	The malware status of the file. Possible values include: • `1` - CLEAN The file is clean and does not contain malware. • `2` - UNKNOWN It is unknown whether the file contains malware. • `3` - MALWARE The file contains malware. • `4` - UNAVAILABLE The software was unable to send a request to the Cisco cloud for a disposition, or the Cisco cloud services did not respond to the request. • `5` - CUSTOM SIGNATURE The file matches a user-defined hash, and is treated in a fashion designated by the user
User Defined	uint8	Indicated how the file name was provided: • `0` - defined by AMP • `1` - user defined

Rule Documentation Data Block for 5.2+

The eStreamer service uses the Rule Documentation data block to contain information about rules used to generate alerts. The block type is 27 in the series 2 set of data blocks. It can be requested with a host request message of type 10. See Host Request Message Format, page 2-24 for more information.

The following diagram shows the structure of a rule documentation data block:

Byte	0								1								2								3							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	Rule Documentation Block Type (27)																															
	Rule Documentation Block Length																															
	Signature ID																															
	Generator ID																															
	Revision																															
Summary	String Block Type (0)																															
	String Block Length																															
	Summary...																															
Impact	String Block Type (0)																															
	String Block Length																															
	Impact...																															
Detailed Info	String Block Type (0)																															
	String Block Length																															
	Detailed Information																															
Affected Systems	String Block Type (0)																															
	String Block Length																															
	Affected Systems...																															
Attack Scenarios	String Block Type (0)																															
	String Block Length																															
	Attack Scenarios...																															

Byte	0								1								2								3							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Ease of Attack	String Block Type (0)																															
	String Block Length																															
	Ease of Attack...																															
False Positives	String Block Type (0)																															
	String Block Length																															
	False Positives...																															
False Negatives	String Block Type (0)																															
	String Block Length																															
	False Negatives...																															
Corrective Action	String Block Type (0)																															
	String Block Length																															
	Corrective Action...																															
Contributors	String Block Type (0)																															
	String Block Length																															
	Contributors...																															
Additional References	String Block Type (0)																															
	String Block Length																															
	Additional References...																															

The following table describes the fields in the rule documentation data block.

Table 3-40 Rule Documentation Data Block Fields

Field	Data Type	Description
Rule Documentation Data Block Type	uint32	Initiates a Rule Documentation data block. This value is always 27.
Rule Documentation Data Block Length	uint32	Total number of bytes in the Rule Documentation data block, including eight bytes for the Rule Documentation data block type and length fields, plus the number of bytes of data that follows.
Rule ID (Signature ID)	uint32	Rule identification number that corresponds with the event.

Table 3-40 Rule Documentation Data Block Fields (continued)

Field	Data Type	Description
Generator ID	uint32	Identification number of the FireSIGHT System preprocessor that generated the event.
Rule Revision	uint32	Rule revision number.
String Block Type	uint32	Initiates a String data block containing the summary associated with the rule. This value is always 0.
String Block Length	uint32	The number of bytes included in the name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Summary field.
Summary	string	Explanation of the threat or vulnerability.
String Block Type	uint32	Initiates a String data block containing the impact associated with the rule. This value is always 0.
String Block Length	uint32	The number of bytes included in the name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Impact field.
Impact	string	How a compromise that uses this vulnerability may impact various systems.
String Block Type	uint32	Initiates a String data block containing the detailed information associated with the rule. This value is always 0.
String Block Length	uint32	The number of bytes included in the name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Detailed Information field.
Detailed Information	string	Information regarding the underlying vulnerability, what the rule actually looks for, and what systems are affected.
String Block Type	uint32	Initiates a String data block containing the list of affected systems associated with the rule. This value is always 0.
String Block Length	uint32	The number of bytes included in the name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Affected Systems field.
Affected Systems	string	Systems affected by the vulnerability.
String Block Type	uint32	Initiates a String data block containing the possible attack scenarios associated with the rule. This value is always 0.
String Block Length	uint32	The number of bytes included in the name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Attack Scenarios field.
Attack Scenarios	string	Examples of possible attacks.
String Block Type	uint32	Initiates a String data block containing the ease of attack associated with the rule. This value is always 0.
String Block Length	uint32	The number of bytes included in the name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Ease of Attack field.
Ease of Attack	string	Whether the attack is considered simple, medium, hard, or difficult, and whether or not is can be performed using a script.

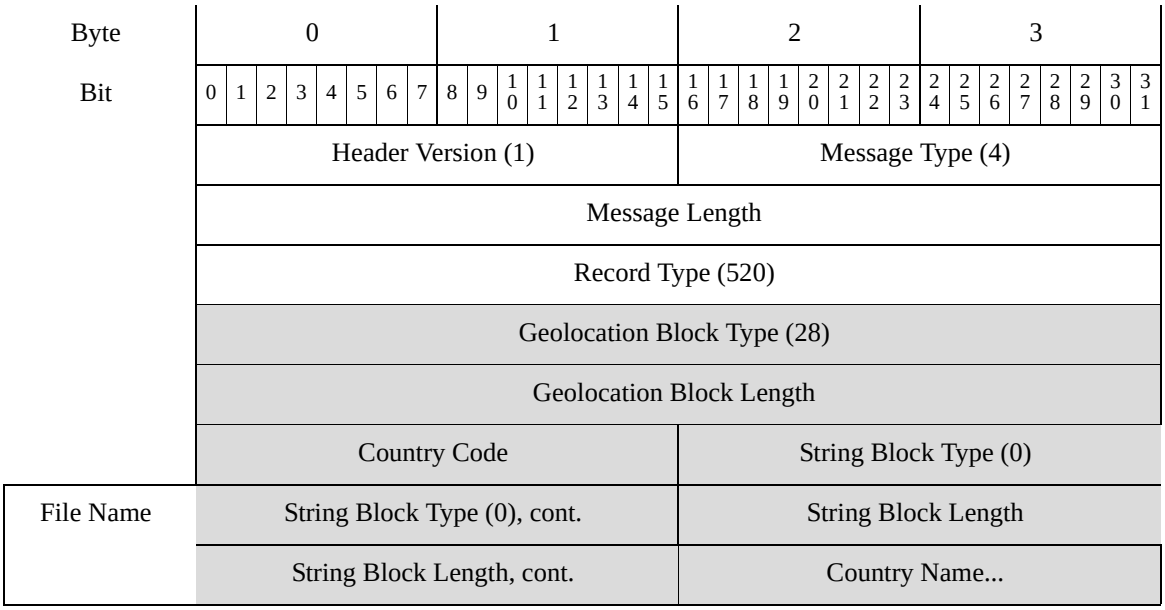
Table 3-40 Rule Documentation Data Block Fields (continued)

Field	Data Type	Description
String Block Type	uint32	Initiates a String data block containing the possible false positives associated with the rule. This value is always 0.
String Block Length	uint32	The number of bytes included in the name String data block, including eight bytes for the block type and header fields plus the number of bytes in the False Positives field.
False Positives	string	Examples that may result in a false positive. The default value is `None Known`.
String Block Type	uint32	Initiates a String data block containing the possible false negatives associated with the rule. This value is always `0`.
String Block Length	uint32	The number of bytes included in the name String data block, including eight bytes for the block type and header fields plus the number of bytes in the False Negatives field.
False Negatives	string	Examples that may result in a false negative. The default value is `None Known`.
String Block Type	uint32	Initiates a String data block containing the corrective action associated with the rule. This value is always `0`.
String Block Length	uint32	The number of bytes included in the name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Corrective Action field.
Corrective Action	string	Information regarding patches, upgrades, or other means to remove or mitigate the vulnerability.
String Block Type	uint32	Initiates a String data block containing the contributors for the rule. This value is always `0`.
String Block Length	uint32	The number of bytes included in the name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Contributors field.
Contributors	string	Contact information for the author of the rule and other relevant documentation.
String Block Type	uint32	Initiates a String data block containing the additional references associated with the rule. This value is always `0`.
String Block Length	uint32	The number of bytes included in the name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Additional References field.
Additional References	string	Additional information and references.

Geolocation Data Block for 5.2+

This is a data block that contains the mapping of a country code to a country name. The record type is 520, and a block type of 28 in series 2. It is exposed as metadata for any event that has geolocation information. If metadata is requested and there is a value for the country code(s) in the event, then this block is returned along with other metadata.

The following diagram shows the structure of a geolocation data block:



The following table describes the fields in the Geolocation data block.

Table 3-41 Geolocation Data Block Fields

Field	Data Type	Description
Geolocation Data Block Type	uint32	Initiates a Geolocation data block. This value is always `28`.
Geolocation Data Block Length	uint32	Total number of bytes in the Geolocation data block, including eight bytes for the Geolocation data block type and length fields, plus the number of bytes of data that follows.
Country Code	uint16	The country code.
String Block Type	uint32	Initiates a String data block containing the country name associated with the country code. This value is always `0`.
String Block Length	uint32	The number of bytes included in the name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Country Name field.
Country Name	string	The name of the country associated with the country code.