

Understanding Legacy Data Structures

This appendix contains information about data structures supported by eStreamer at previous versions of FireSIGHT System products.

If your client uses event stream requests with bits set to request data in older version formats, you can use the information in this appendix to identify the data structures of the data messages you receive.

Note that prior to version 5.0, separate detection engines were assigned IDs. For version 5.0, devices are assigned IDs. Based on the version, data structures reflect this.



This appendix describes only data structures from version 4.9 or later of the FireSIGHT System. If you require documentation for structures from earlier data structure versions, contact Cisco Customer Support.

See the following sections for more information:

- Legacy Intrusion Data Structures, page B-1
- Legacy Malware Event Data Structures, page B-38
- Legacy Discovery Data Structures, page B-69
- Legacy Connection Data Structures, page B-92
- Legacy File Event Data Structures, page B-129
- Legacy Correlation Event Data Structures, page B-151
- Legacy Host Data Structures, page B-166

Legacy Intrusion Data Structures

- Intrusion Event (IPv4) Record 5.0.x 5.1, page B-2
- Intrusion Event (IPv6) Record 5.0.x 5.1, page B-6
- Intrusion Event Record 5.2.x, page B-12
- Intrusion Event Record 5.3, page B-17
- Intrusion Event Record 5.1.1.x, page B-23
- Intrusion Event Record 5.3.1, page B-29
- Intrusion Impact Alert Data, page B-36

Intrusion Event (IPv4) Record 5.0.x - 5.1

The fields in the intrusion event (IPv4) record are shaded in the following graphic. The record type is 207.

You request intrusion event records by setting the intrusion event flag or the extended requests flag in the request message. See Request Flags, page 2-11 and Submitting Extended Requests, page 2-4.

For version 5.0.x - 5.1 intrusion events, the event ID, the managed device ID, and the event second form a unique identifier.

By te	0	1	2	3	
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 3 3 3 4 5 6 7 8 9 0 1	
	Header Ve	ersion (1)	Message	Type (4)	
		Message	Length		
		Record Ty	ype (207)		
		Record	Length		
	eStream	ner Server Timestamp (in events, only if bit 23	3 is set)	
	Reser	ved for Future Use (in	events, only if bit 23 is	s set)	
	Device ID				
	Event ID				
		Event S	Second		
		Event Mic	crosecond		
		Rule ID (Sig	gnature ID)		
		Genera	ntor ID		
		Rule Re	evision		
		Classific	ation ID		
		Priori	ty ID		
	Source IPv4 Address				
	Destination IPv4 Address				
	Source Port Destination Port			ion Port	
	IP Protocol ID	Impact Flags	Impact	Blocked	
		MPLS	Label		

By te	0	1	2	3		
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1		
	VLAN	N ID	P	ad		
		Policy	UUID			
		Policy UUIE	O, continued			
		Policy UUID), continued			
		Policy UUID), continued			
		User	r ID			
		Web Appli	ication ID			
		Client App	lication ID			
		Application	Protocol ID			
	Access Control Rule ID					
		Access Control	l Policy UUID			
		Access Control Police	cy UUID, continued			
		Access Control Police	cy UUID, continued			
		Access Control Police	cy UUID, continued			
		Interface Ing	gress UUID			
		Interface Ingress	UUID, continued			
		Interface Ingress	UUID, continued			
		Interface Ingress	UUID, continued			
		Interface Eg	gress UUID			
		Interface Egress U	UUID, continued			
		Interface Egress U	UUID, continued			
		Interface Egress U	UUID, continued			
	Security Zone Ingress UUID					
		Security Zone Ingres	ss UUID, continued			
		Security Zone Ingres	ss UUID, continued			

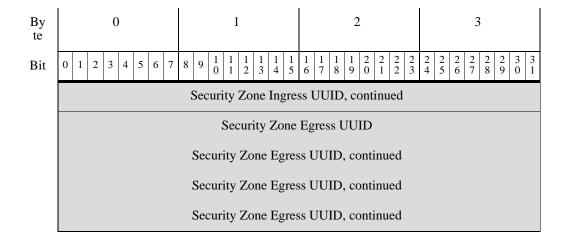


Table B-1 Intrusion Event (IPv4) Record Fields

Field	Data Type	Description
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 3-32 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 IPv4 Address	uint8[4]	Source IPv4 address used in the event, in address octets.
Destination IPv4 Address	uint8[4]	Destination IPv4 address used in the event, in address octets.
Source Port	uint16	The source port number if the event protocol type is TCP or UDP.
Destination Port	uint16	The destination port number if the event protocol type is TCP or UDP.

Table B-1 Intrusion Event (IPv4) Record Fields (continued)

Field	Data Type	Description
IP Protocol	uint8	IANA-specified protocol number. For example:
Number		• 0 — IP
		• 1 — ICMP
		• 6 — TCP
		• 17 — UDP
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.
		The following impact level values map to specific priorities on the Defense Center. An x indicates the value can be 0 or 1:
		• (0, unknown): 00x00000
		• red (1, vulnerable): xxxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx
		• orange (2, potentially vulnerable): 00x00111
		• yellow (3, currently not vulnerable): 00x00011
		• blue (4, unknown target): 00x00001

Table B-1 Intrusion Event (IPv4) Record Fields (continued)

Field	Data Type	Description			
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 — (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)			
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.			

Intrusion Event (IPv6) Record 5.0.x - 5.1

The fields in the intrusion event (IPv6) record are shaded in the following graphic. The record type is 208.

You request intrusion event records by setting the intrusion event flag or the extended requests flag in the request message. See Request Flags, page 2-11 and Submitting Extended Requests, page 2-4.

For version 5.0.x - 5.1 intrusion events, the event ID, the managed device ID, and the event second form a unique identifier.

By te	0	1	2	3	
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1	
	Header Version (1) Message Type (4)				
		Message	Length		
		Record Ty	rpe (208)		
		Record	Length		
	eStrean	ner Server Timestamp (in events, only if bit 2	3 is set)	
	Rese	rved for Future Use (in	events, only if bit 23 i	s set)	
		Devid	ce ID		
		Even	t ID		
	Event Second				
	Event Microsecond				
		Rule ID (Sig	gnature ID)		
		Genera	tor ID		
		Rule Re	evision		
		Classifica	ation ID		
		Priorit	ty ID		
		Source IPv	6 Address		
		Source IPv6 Add	lress, continued		
		Source IPv6 Add	lress, continued		
	Source IPv6 Address, continued				
		Destination II	Pv6 Address		
		Destination IPv6 A	ddress, continued		
		Destination IPv6 A	ddress, continued		

By te	0	1	2 3			3								
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1	1 1 5 6	l 1 5 7	1 1 8 9	2 0	2	2 2 3	2 4	2 2 6	2 7	2 2 9	3	3
		Destination IPv6	Ad	ldres	s, co	ntin	ued							
	Source Port/	ICMP Type			De	estin	atio	n Po	rt/IC	СМР	Co	de		
	IP Protocol ID Impact Flags Impact Blocked				Ī									
		MPL	SL	Label										
	VLAN ID Pad													
		Polic	y U	UID)									
		Policy UU	ID,	con	tinue	d								
		Policy UU	ID,	con	tinue	ed								
		Policy UU	ID,	con	tinue	d								
		Us	er l	ID										
		Web App	plic	atior	ı ID									
		Client Ap	plio	catio	n ID)								
		Applicatio	n P	roto	col II	D								
		Access Co	ntro	ol Ru	ıle II	D								
		Access Contr	ol I	Polic	y Ul	UID)							
		Access Control Po	licy	' UU	TD,	cont	inue	ed						
		Access Control Po	licy	' UU	TD,	cont	inue	ed						
		Access Control Po	licy	' UU	ID,	cont	inue	ed						
		Interface I	ngr	ess I	JUII)								
		Interface Ingres	s U	UID	, cor	ntinu	ied							
	Interface Ingress UUID, continued													
	Interface Ingress UUID, continued													
	Interface Egress UUID													
		Interface Egress	s U	UID.	, con	tinu	ied							
		Interface Egress	s U	UID.	, con	tinu	ied							

By te	0	1	2	3			
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 3 3 4 5 6 7 8 9 0 1			
		Interface Egress U	UUID, continued				
		Security Zone	Ingress UUID				
		Security Zone Ingres	ss UUID, continued				
	Security Zone Ingress UUID, continued						
	Security Zone Ingress UUID, continued						
	Security Zone Egress UUID						
		Security Zone Egres	ss UUID, continued				
		Security Zone Egres	ss UUID, continued				
		Security Zone Egres	ss UUID, continued				

Table B-2 Intrusion Event (IPv6) Record Fields

Field	Data Type	Description
Device ID	unit32	Contains the identification number of the detecting device. You can obtain the managed device name by requesting Version 3 or 4 metadata. See Managed Device Record Metadata, page 3-32 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 IPv6 Address	uint8[16]	Source IPv6 address used in the event, in address octets.
Destination IPv6 Address	uint8[16]	Destination IPv6 address used in the event, in address octets.

Table B-2 Intrusion Event (IPv6) Record Fields (continued)

Field	Data Type	Description
Source Port/ICMP Type	uint16	The source port number if the event protocol type is TCP or UDP. If the protocol type is ICMP, this indicates the ICMP type.
Destination Port/ICMP Code	uint16	The destination port number if the event protocol type is TCP or UDP. If the protocol type is ICMP, this indicates the ICMP code.
IP Protocol Number	uint8	IANA-specified protocol number. For example: • 0 — IP • 1 — ICMP • 6 — TCP • 17 — UDP
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. The following impact level values map to specific priorities on the Defense Center. An x indicates the value can be 0 or 1: (0, unknown): 00x000000 red (1, vulnerable): xxxxx1xxx, xxxx1xxxx, x1xxxxxx, 1xxxxxxxx

Table B-2 Intrusion Event (IPv6) Record Fields (continued)

Field	Data Type	Description
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 — (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)
MPLS Label	uint32	MPLS label. (Applies to 4.9+ events only.)
VLAN ID	uint16	Indicates the ID of the VLAN where the packet originated. (Applies to 4.9+ events only.)
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.

Intrusion Event Record 5.2.x

The fields in the intrusion event record are shaded in the following graphic. The record type is 400 and the block type is 34 in the series 2 set of data blocks.

You can request 5.2.x intrusion events from eStreamer only by extended request, for which you request event type code 12 and version code 5 in the Stream Request message (see Submitting Extended Requests, page 2-4 for information about submitting extended requests).

For version 5.2.x 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 1 1 1 1 1 1 1 5	1 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1		
	Header Ve	ersion (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 (34)					
		Block I	Length			
		Devic	ce ID			
		Even	t ID			
		Event S	Second			
		Event Mic	crosecond			
		Rule ID (Sig	gnature ID)			
		Genera	tor ID			
	Rule Revision					
	Classification ID					
		Priori	ty ID			

Byte	0	1	2 3										
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1									
	Source IP Address												
	Source IP Address, continued												
	Source IP Address, continued												
	Source IP Address, continued												
	Destination IP Address												
		Destination IP A	ddress, continued										
		Destination IP A	ddress, continued										
	Destination IP Address, continued												
	Source Port or ICMP Type Destination Port or ICMP Code												
	IP Protocol ID	Impact Flags	Impact	Blocked									
		MPLS	Label										
	VLA	N ID	Pa	ad									
		Policy	UUID										
	Policy UUID, continued												
		Policy UUII	O, continued										
		Policy UUII	O, continued										
		Use	r ID										
		Web Appl	ication ID										
		Client App	lication ID										
		Application	Protocol ID										
		Access Con	trol Rule ID										
		Access Contro	l Policy UUID										
		Access Control Police	cy UUID, continued										
		Access Control Police	cy UUID, continued										
		Access Control Police	cy UUID, continued										
		Interface In	gress UUID										

Byte	0 1 2 3												
Bit	0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1												
	Interface Ingress UUID, continued												
	Interface Ingress UUID, continued												
	Interface Ingress UUID, continued												
	Interface Egress UUID												
		Interface Egress U	JUID, continued										
		Interface Egress U	JUID, continued										
	Interface Egress UUID, continued												
	Security Zone Ingress UUID												
		Security Zone Ingress UUID, continued											
	Security Zone Ingress UUID, continued												
		Security Zone Ingress UUID, continued											
		Security Zone	Egress UUID										
		Security Zone Egres	ss UUID, continued										
		Security Zone Egres	ss UUID, continued										
		Security Zone Egress UUID, continued											
	Connection Timestamp												
	Connection	Instance ID	Connection	n Counter									
	Source (Country	Destination	n Country									

Table B-3 Intrusion Event Record 5.2.x Fields

Field	Data Type	Description Initiates an Intrusion Event data block. This value is always 34.						
Block Type	unint32							
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 3-32 for more information.						

Table B-3 Intrusion Event Record 5.2.x Fields (continued)

Field	Data Type	Description							
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 B-3 Intrusion Event Record 5.2.x 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:
		• (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): 00x000001
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 — (unknown impact)
Blocked	uint8	Value indicating whether the event was blocked.
		• 0 — Not blocked
		• 1 — Blocked

Table B-3 Intrusion Event Record 5.2.x 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	uint 16	Code for the country of the destination host.

Intrusion Event Record 5.3

The fields in the intrusion event record are shaded in the following graphic. The record type is 400 and the block type is 41 in the series 2 set of data blocks.

You can request 5.3 intrusion events from eStreamer only by extended request, for which you request event type code 12 and version code 6 in the Stream Request message (see Submitting Extended Requests, page 2-4 for information about submitting extended requests).

For version 5.3 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 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1					
	Header Version (1) Message Type (4)								
		Message	Length						
		Record Ty	pe (400)						
		Record I	Length						
	eStream	ner Server Timestamp (i	n events, only if bit 23	3 is set)					
	Reser	rved for Future Use (in	events, only if bit 23 is	s set)					
		Block Ty	pe (41)						
		Block Length							
		Device ID							
		Event	: ID						
		Event S	econd						
		Event Mic	rosecond						
		Rule ID (Sig	gnature ID)						
		Generat	tor ID						
		Rule Re	vision						
		Classifica	ation ID						
		Priority ID							
		Source IP Address							
		Source IP Addre							
		Source IP Addre							
		Source IP Addre	ess, continued						

Byte	0									1							2								3							
Bit	0 1	2	3	4	5	6	5 7	8	ç	$9 \begin{vmatrix} 1 \\ 0 \end{vmatrix}$	1	1 2	1 1 2 3	1 4	1 5	1 6	1 7		1 1 8 9	2	1	2 2 1 2	2 3		2 4	$\begin{bmatrix} 2 & 2 \\ 5 & \epsilon \end{bmatrix}$	5	2 7	2 2 9	3 3 0 1		
		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																														
	Ι	IP Protocol ID Impact Flags Impact Blocked																														
]	MP	LS	S La	be	1														
						V	/LA	ΝI	ID)													Pa	ac	i							
		Policy UUID																														
		Policy UUID, continued																														
											P	o	licy	U	JI	D, c	con	ıti	nue	d												
											P	o	licy	U	JI	D, 0	con	ıti	nue	d												
														U	Jse	er II)															
												1	Web	A _l	op	lica	tio	n	ID													
												C	Clier	nt A	p	plica	atio	on	ID													
											A	٩ŗ	opli	cati	or	Pro	oto	C	ol II)												
											F	40	cces	s C	OI	ntro	l R	ul	le II)												
																ol P		Ī														
										cces						-																
										cces																						
								1	A	cces											tiı	nue	d —									
																igre																
														_		UU																
														_		UU																
										Inte				_		UU					ue	ed										
]	In	iterf	ace	E	gre	ss l	U	UII)												

Byte	0	1	2	3								
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1								
	Interface Egress UUID, continued											
	Interface Egress UUID, continued											
		Interface Egress UUID, continued										
		Security Zone	Ingress UUID									
		Security Zone Ingre	ss UUID, continued									
	Security Zone Ingress UUID, continued											
		Security Zone Ingre	ss UUID, continued									
		Security Zone Egress UUID										
		Security Zone Egre	ss UUID, continued									
		Security Zone Egre	ss UUID, continued									
		Security Zone Egre	ss UUID, continued									
		Connection	Timestamp									
	Connection	Instance ID	Connectio	n Counter								
	Source (Country	Destinatio	n Country								
	IOC N	umber										

Table B-4 Intrusion Event Record 5.3 Fields

Field	Data Type	Description			
Block Type	unint32	Initiates an Intrusion Event data block. This value is always 34.			
Block Length unint32 Total number of bytes in the Intrusion Event data block, incl eight bytes for the Intrusion Event block type and length fiel 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 3-32 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.			

Table B-4 Intrusion Event Record 5.3 Fields (continued)

Field	Data Type	Description					
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 B-4 Intrusion Event Record 5.3 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:
		• (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 — (unknown impact)
Blocked	uint8	Value indicating whether the event was blocked.
		• 0 — Not blocked
		• 1 — Blocked
	1	

Table B-4 Intrusion Event Record 5.3 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	uint 16	Code for the country of the destination host.
IOC Number	uint16	ID Number of the compromise associated with this event.

Intrusion Event Record 5.1.1.x

The fields in the intrusion event record are shaded in the following graphic. The record type is 400 and the block type is 25.

You can request 5.1.1.x intrusion events from eStreamer only by extended request, for which you request event type code 12 and version code 4 in the Stream Request message (see Submitting Extended Requests, page 2-4 for information about submitting extended requests).

For version 5.1.1.x 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.

0	1	2	3							
0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1							
Header Version (1) Message Type (4)										
	Message	Length								
	Record Ty	rpe (400)								
	Record l	Length								
eStream	ner Server Timestamp (i	n events, only if bit 23	3 is set)							
Reser	ved for Future Use (in	events, only if bit 23 i	s set)							
	Block Ty	rpe (25)								
	Block I	ength								
	Devic	e ID								
	Even	t ID								
	Event S	econd								
	Event Mic	rosecond								
	Rule ID (Sig	gnature ID)								
	Genera	tor ID								
	Rule Re	vision								
	Classifica	ation ID								
	Priorit	y ID								
	Source IP	Address								
	Source IP Addr	ess, continued								
	Source IP Addr	ess, continued								
	Source IP Addr	ess, continued								
	0 1 2 3 4 5 6 7 Header Vo	Message Record Ty Record I Reserved for Future Use (in Block I Device Event S Event Mic Rule ID (Sig General Rule Re Classifica Priorit Source IP Addr Source IP Addr Source IP Addr	0 1 2 3 4 5 6 7 8 9 1 1 2 3 4 5 6 7 8 9 2 3 4 5 6 7 8 9 3 3 4 5 6 7 8 9 3 3 4 5 6 7 8 9 3 3							

By te	0	1	2	3									
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1									
		Destination	IP Address										
		Destination IP Address, continued											
		Destination IP Ad	ldress, continued										
		Destination IP Ac	ldress, continued										
	Source Port/ICMP Type Destination Port/ICMP Code												
	IP Protocol ID Impact Flags Impact Blocked												
		MPLS	Label										
	VLA	N ID	Pa	nd									
		Policy	UUID										
		Policy UUID	O, continued										
		Policy UUID	O, continued										
		Policy UUID	O, continued										
		User	· ID										
		Web Appli	ication ID										
		Client App	lication ID										
		Application	Protocol ID										
		Access Cont	trol Rule ID										
		Access Control	Policy UUID										
		Access Control Police	cy UUID, continued										
		Access Control Police	cy UUID, continued										
		Access Control Police	cy UUID, continued										
		Interface Ing	gress UUID										
		Interface Ingress	UUID, continued										
		Interface Ingress	UUID, continued										
		Interface Ingress	UUID, continued										

By te	0	1	2	3							
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1							
		Interface Eg	gress UUID								
		Interface Egress UUID, continued									
		Interface Egress U	JUID, continued								
		Interface Egress U	JUID, continued								
		Security Zone Ingress UUID									
		Security Zone Ingres	ss UUID, continued								
		Security Zone Ingres	ss UUID, continued								
		Security Zone Ingres	ss UUID, continued								
	Security Zone Egress UUID										
	Security Zone Egress UUID, continued										
		Security Zone Egres	ss UUID, continued								
		Security Zone Egress UUID, continued									
		Connection	Timestamp								
	Connection	Instance ID	Connection	n Counter							

Table B-5 Intrusion Event Record 5.1.1 Fields

Field	Data Type	Description
Block Type	unint32	Initiates an Intrusion Event data block. This value is always 25.
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 3-32 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.

Table B-5 Intrusion Event Record 5.1.1 Fields (continued)

Field	Data Type	Description
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/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/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 B-5 Intrusion Event Record 5.1.1 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.
		The following impact level values map to specific priorities on the Defense Center. An x indicates the value can be 0 or 1:
		• (0, unknown): 00x00000
		• red (1, vulnerable): xxxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx
		• orange (2, potentially vulnerable): 00x00111
		• yellow (3, currently not vulnerable): 00x00011
		• 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 — (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 B-5 Intrusion Event Record 5.1.1 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.

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	1 5	6	7	8	9	1 1	l L	1 1 2 3	1 4	1 5	1 1	1 7	1 8	1 2	2	2 2 3		2 4	2 2 5 6	2 7	2 2 9	3 0	3
	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)																									
											Bl	lock	Ту	pe ((4:	2)										
											I	Bloo	ck I	Leng	ţtŀ	1										
												De	evic	e II)											
												E	ven	t ID												
											I	Eve	nt S	eco	nc	1										
											Eve	nt l	Mic	rose	cc	ond										
										F	Rule	ID	(Sig	gnati	ur	e II))									
														tor l												
														visi												
											Cl			ation		ID										
														y II												
									C-					Ado				.1								
											rce II rce II															
											rce II															
								Г	4		Desti															
											atior atior															
											ation															
									_50		01					, 501										

Byte	0	1	2	3						
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 3 3 6 7 8 9 0 1 1 2 3 4 5 6 7 8 9 0 1							
	Source Port o	r ICMP Type	Destination Port or ICMP Code							
	IP Protocol ID Impact Flags Impact Blocked									
		MPLS	Label							
	VLA	N ID	Pa	ıd						
		Policy	UUID							
		Policy UUID), continued							
		Policy UUID), continued							
		Policy UUID								
		User								
		Web Appli								
		Client Appl								
		Application								
		Access Control								
		Access Control Police	•							
		Access Control Police								
		Access Control Police								
		Interface Ing								
		Interface Ingress I								
		Interface Ingress V	JUID, continued							
		Interface Ingress I	UUID, continued							
		Interface Eg	ress UUID							
		Interface Egress U	JUID, continued							
		Interface Egress U	JUID, continued							
		Interface Egress U	JUID, continued							
		Security Zone	Ingress UUID							

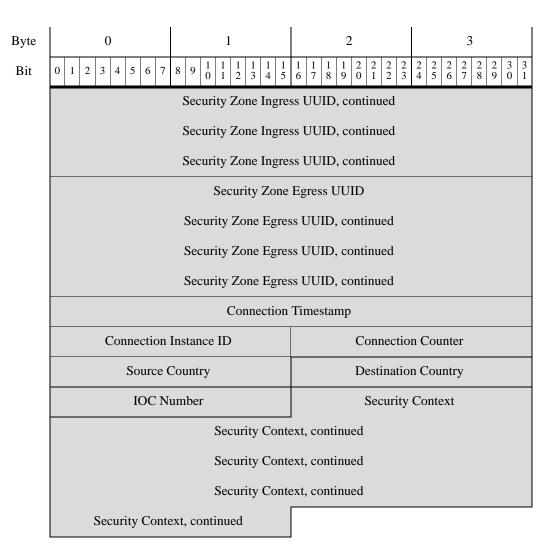


Table B-6 Intrusion Event Record 5.3.1 Fields

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 3-32 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.

Table B-6 Intrusion Event Record 5.3.1 Fields (continued)

Field	Data Type	Description						
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 B-6 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:		
		• (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 — (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 B-6 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	uint 16	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

ı

The Intrusion Impact Alert 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 data block type of 20 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 4-54.)

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 1 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1			
	Header Ve	Type (4)					
	Message Length						
	Record Type (9) Record Length Intrusion Impact Alert Block Type (20) Intrusion Impact Alert Block Length Event ID						
	Device ID						
	Event Second						
	Impact						
	Source IP Address						
	Destination IP Address						
Impact Description	String Block Type (0)						
	String Block Length						
	Description						

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

Table B-7 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.
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:
		• (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

Table B-7 Impact Event Data Fields (continued)

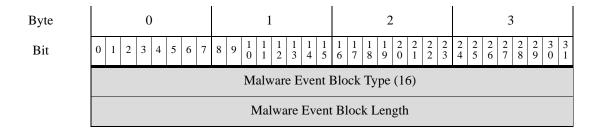
Field	Data Type	Description
Source IP Address	uint8[4]	IP address of the host associated with the impact event, in IP address octets.
Destination IP Address	uint8[4]	IP address of the destination IP address associated with the impact event (if applicable), in IP address octets. This value is 0 if there 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 4-62.
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.

Legacy Malware Event Data Structures

- Malware Event Data Block 5.1, page B-38
- Malware Event Data Block 5.1.1.x, page B-42
- Malware Event Data Block 5.2.x, page B-48
- Malware Event Data Block 5.3, page B-55
- Malware Event Data Block 5.3.1, page B-62

Malware Event Data Block 5.1

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 16 in the series 2 group of blocks. 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 1 and an event code of 101.



Byte	0	1	2	3
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1
		Agent	UUID	
	Agent UUID, continued Agent UUID, continued			
		Agent UUID), continued	
		Cloud	UUID	
		Cloud UUID), continued	
		Cloud UUID), continued	
		Cloud UUIE), continued	
		Times	stamp	
	Event Type ID			
	Event Subtype ID		Host IP Address	
Detection Name	Host IP Address, cont.	Detector ID	String Blo	ck Type (0)
	String Block Type (0), cont.		String Blo	ock Length
	String Block	Length, cont.	Detectio	n Name
User		String Bloc	k Type (0)	
		String Blo	ck Length	
	User			
File Name		String Bloc	ek Type (0)	
	String Block Length			
		File N	ame	
File Path St		String Bloc	ek Type (0)	
		String Blo	ck Length	
		File P	ath	

Byte	0	1	2	3
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 3 3 4 5 6 7 8 9 0 1
File SHA Hash	String Block Type (0)			
11451		String Block Length		
		File SHA	Hash	
		File S	Size	
	File Type		File Timestamp	
Parent File Name	File Timestamp, cont.		String Block Type (0)	
	String Block Type (0), cont.		String Block Length	
	String Block Length, cont.		Parent File Name	
Parent File SHA Hash		String Block Type (0)		
SHATIUSH	String Block Length			
	Parent File SHA Hash			
Event Description	String Block Type (0)			
	String Block Length			
		Event Des	cription	

Table B-8 Malware Event Data Block Fields

Field	Data Type	Description
Malware Event Block Type	uint32	Initiates a malware event data block. This value is always 16.
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 malware awareness network from which the malware event originated.
Timestamp	uint32	The malware event generation timestamp.
Event Type ID	uint32	The internal ID of the malware event type.

Table B-8 Malware Event Data Block Fields (continued)

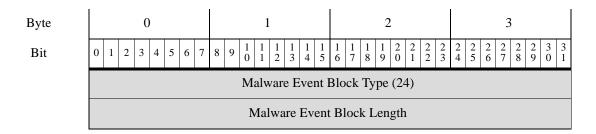
Field	Data Type	Description
Event Subtype ID	uint8	The internal ID of the action that led to malware detection.
Host IP Address	uint32	The host IP address associated with the malware event.
Detector ID	uint8	The internal ID of the detection technology that detected the malware.
String Block Type	uint32	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.
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 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	uint8	The file type of the detected or quarantined file.
File Timestamp	uint32	The creation timestamp of the detected or quarantined file.

Table B-8 Malware Event Data Block Fields (continued)

Field	Data Type	Description
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.
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.

Malware Event Data Block 5.1.1.x

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 24 in the series 2 group of blocks. 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 2 and an event code of 101.



Byte	0	1	2	3
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1
		Agent	UUID	
		Agent UUID, continued		
	Agent UUID, continued			
		Agent UUID	O, continued	
		Cloud	UUID	
		Cloud UUIE	O, continued	
		Cloud UUIE	O, continued	
		Cloud UUID), continued	
		Malware Ever	nt Timestamp	
	Event Type ID			
	Event Subtype ID		Host IP Address	
Detection Name	Host IP Address, cont.	Detector ID	String Block Type (0)	
	String Block Type (0), cont.		String Blo	ock Length
	String Block	Length, cont.	Detection	on Name
User		String Bloc	ek Type (0)	
		String Blo	ck Length	
	User			
File Name		String Bloc	ek Type (0)	
	String Block Length			
		File N	ame	
File Path		String Bloc	k Type (0)	
		String Blo	ck Length	
		File P	ath	

Byte	0	1	2 3	ĺ
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 3 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0	3
File SHA	String Block Type (0)			
Hash	String Block Length			
		File SHA	A Hash	
	File Size			
	File Type		File Timestamp	
Parent File Name	File Timestamp, cont.		String Block Type (0)	
	String Block Type (0), cont.		String Block Length	
	String Block Length, cont.		Parent File Name	
Parent File SHA Hash		String Bloc	ek Type (0)	
SIIIIII		String Blo	ck Length	
	Parent File SHA Hash			
Event Description	String Block Type (0)			
2 comption	String Block Length			
	Event Description			
		Devid	ce ID	
	Connection	n Instance	Connection Counter	
		Connection Ev	ent Timestamp	
	Direction		Source IP Address	
		Source IP Adda		
	Source IP Address, continued			
		Source IP Addi	ress, continued	
	Source IP, cont.		Destination IP Address	
		Destination IP Ac		
		Destination IP Ac		
		Destination IP Ac	idress, continued	

Byte	0	1	2	3
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1
	Destination IP,		Application ID	
	App. ID, cont.		User ID	
	User ID, cont.	Acc	cess Control Policy UU	JID
		Access Control Police	cy UUID, continued	
		Access Control Police	cy UUID, continued	
		Access Control Police	cy UUID, continued	
URI	AC Pol UUID, cont.	Disposition	Retro. Disposition	Str. Block Type (0)
	Strin	g Block Type (0), conti	nued	String Block Length
	Strir	g Block Length, contin	nued	URI
	Sourc	e Port	Destinat	ion Port

Table B-9 Malware Event Data Block for 5.1.1.x Fields

Field	Data Type	Description
Malware Event Block Type	uint32	Initiates a malware event data block. This value is always 24.
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 malware awareness network 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	uint8	The internal ID of the action that led to malware detection.
Host IP Address	uint32	The host IP address associated with the malware event.
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.

Table B-9 Malware Event Data Block for 5.1.1.x Fields (continued)

Field	Data Type	Description	
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.	
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	uint8	The file type of the detected or quarantined file.	
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.	

Table B-9 Malware Event Data Block for 5.1.1.x Fields (continued)

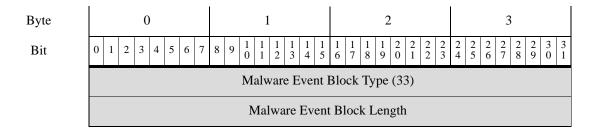
Field	Data Type	Description
String Block Length	uint32	The number of bytes included in the Parent File Name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Parent File Name field.
Parent File Name	string	The name of the file accessing the 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.
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.

Table B-9 Malware Event Data Block for 5.1.1.x Fields (continued)

Field	Data Type	Description						
Access Control Policy UUID	uint8[16]	Identification number that acts as a unique identifier for the access control policy that triggered the event.						
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 — CACHE_MISS — The software was unable to send a request to the Cisco cloud for a disposition.						
		• 5 — NO_CLOUD_RESP — The Cisco cloud services did not respond to the request.						
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.						

Malware Event Data Block 5.2.x

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 33 in the series 2 group of blocks. 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 3 and an event code of 101.



Byte	0	1	2	3										
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1										
		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 T	ype ID											
Detection Name	Event Subtype ID	Detector ID	String Bloc	k Type (0)										
	String Block 7	Type (0), cont.	String Blo	ck Length										
	String Block	Length, cont.	Detection	Name										
User		String Bloc	k Type (0)											
		String Bloo	ck Length											
		Use	er											
File Name		String Bloc	k Type (0)											
		String Bloo												
		File N	ame											
File Path		String Bloc												
		String Blo												
		File P												
File SHA Hash		String Bloc												
		String Blo												
		File SHA												
		File	Size											

Byte	0	1	2 3										
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	1 1 2 3 3 8 9 0 1 1 2 3 4 5 6 7 8 9 0 1									
	File Type												
	File Timestamp												
Parent File Name	String Block Type (0)												
Tvame	String Block Length												
	Parent File Name												
Parent File SHA Hash	String Block Type (0)												
SINTINGN		String Blo	ck Length										
		Parent File S	SHA Hash										
Event Description		String Bloo	ck Type (0)										
T. T.		String Blo	ck Length										
	Event Description												
		Devi	ce ID										
	Connection	n Instance	Connection	on Counter									
		Connection Ev	nt Timestamp										
	Direction		Source IP Address										
		Source IP Add											
		Source IP Add											
		Source IP Add	ress, continued										
	Source IP, cont.		Destination IP Address	S									
		Destination IP A											
		Destination IP A											
	Destination IP Address, continued												
	Destination IP, cont Application ID												
	App. ID, cont.		User ID										
	User ID, cont.	Aco	cess Control Policy UU	ЛD									

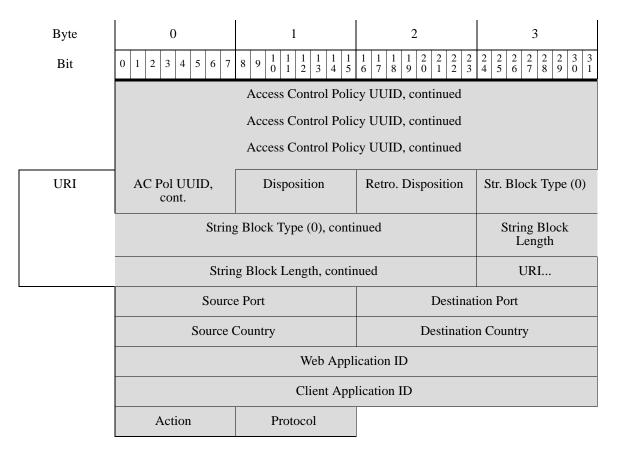


Table B-10 Malware Event Data Block for 5.2.x Fields

Field	Data Type	Description
Malware Event Block Type	uint32	Initiates a malware event data block. This value is always 33.
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 malware awareness network 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	uint8	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.

Table B-10 Malware Event Data Block for 5.2.x Fields (continued)

Field	Data Type	Description					
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.					
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.					
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.					

Table B-10 Malware Event Data Block for 5.2.x Fields (continued)

Field	Data Type	Description
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.
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.

Table B-10 Malware Event Data Block for 5.2.x Fields (continued)

Field	Data Type	Description							
Access Control Policy UUID	uint8[16]	Identification number that acts as a unique identifier for the access control policy that triggered the event.							
Disposition	uint8	The malware status of the file. Possible values include:							
		• 1 — CLEAN — The file is clean and does not contain malware.							
		• 2 — NEUTRAL — It is unknown whether the file contains malware.							
		• 3 — MALWARE — The file contains malware.							
		• 4 — CACHE_MISS — 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.							
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.							

Table B-10 Malware Event Data Block for 5.2.x Fields (continued)

Field	Data Type	Description						
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						
Protocol	uint8	IANA protocol number specified by the user. For example:						
		• 1 — ICMP						
		• 4 — IP						
		• 6 — TCP						
		• 17 — UDP						
		This is currently only TCP.						

Malware Event Data Block 5.3

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 35 in the series 2 group of blocks. 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 4 and an event code of 101.

Byte				C)				1								2							3							
Bit	0	1	2	3	4	5	6	7	8	9	1 0	1	1 2	1 3	1 4	1 5	1	1 7	1 8	1 9	2	2	2 2	2 3	2 4	2 5	2 6	2 7	2 8	2 9	3 3 0 1
	Malware Event Block Type (35)																														
		Malware Event Block Length																													
	Agent UUID																														
												A	Age	ent	UU	JID), c	on	tin	ued	l										
												A	Age	ent	UU	JID), c	on	tin	ued	l										
												Α	Age	ent	UU	JID), c	on	tin	ued	l										
	Cloud UUID																														
												C	Clo	ud	UU	JID), c	on	tin	ued	l										

Byte	0	1	2	3										
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 3 3 4 5 6 7 8 9 0 1										
	Cloud UUID, continued													
	Cloud UUID, continued													
	Malware Event Timestamp													
		Event 7	Type ID											
	Event Subtype ID													
Detection Name	Detector ID		String Block Type (0)											
rume	String Block Type (0), cont.		String Block Length											
	String Block Length, cont.		Detection Name											
User		String Bloo	ck Type (0)											
		String Blo	ck Length											
		Use	er											
File Name		String Bloo	ck Type (0)											
		String Blo	ck Length											
		File N	ame											
File Path		String Bloo	ck Type (0)											
		String Blo	ck Length											
		File F	Path											
File SHA Hash		String Bloo	ck Type (0)											
		String Blo	ck Length											
		File SHA	A Hash											
		File	Size											
		File	Туре											
		File Tin	nestamp											

Byte	0	1	2	3											
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 3 4 5 6 7 8 9 0 1											
Parent File Name		String Bloo	ck Type (0)												
Name	String Block Length														
		Parent File Name													
Parent File SHA Hash	String Block Type (0)														
SIII I II III	String Block Length														
	Parent File SHA Hash														
Event Description	String Block Type (0)														
2 computer		String Block Length													
		Event Des	scription												
	Device ID														
	Connectio	n Instance	Connection	on Counter											
		Connection Ev	ent Timestamp												
	Direction		Source IP Address												
		Source IP Add	ress, continued												
		Source IP Add	ress, continued												
		Source IP Add	ress, continued												
	Source IP, cont.		Destination IP Addres	s											
		Destination IP A	ddress, continued												
		Destination IP A	ddress, continued												
		Destination IP A	ddress, continued												
	Destination IP, cont		Application ID												
	App. ID, cont.		User ID												
	User ID, cont.	Ace	cess Control Policy U	UID											

Byte	0	1	2	3
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1
		Access Control Police	cy UUID, continued	
		Access Control Police	cy UUID, continued	
		Access Control Police	cy UUID, continued	
URI	AC Pol UUID, cont.	Disposition	Retro. Disposition	Str. Block Type (0)
	String	g Block Type (0), conti	nued	String Block Length
	Strin	g Block Length, contin	nued	URI
	Source Port Destination Port			
	Source Country Destination Country			n Country
	Web Application ID			
	Client Application ID			
	Action	Protocol	Threat Score	IOC Number
	IOC Number, cont.			

Table B-11 Malware Event Data Block for 5.3 Fields

Field	Data Type	Description
Malware Event Block Type	uint32	Initiates a malware event data block. This value is always 35.
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 malware awareness network 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.

Table B-11 Malware Event Data Block for 5.3 Fields (continued)

Field	Data Type	Description	
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.	
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 o 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 thi event. See FireAMP File Type Metadata, page 3-37 for morinformation.	
File Timestamp	uint32	UNIX timestamp (seconds since 01/01/1970) of the creation of the detected or quarantined file.	

Table B-11 Malware Event Data Block for 5.3 Fields (continued)

Field	Data Type	Description	
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.	
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	
	1054.67	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.	

Table B-11 Malware Event Data Block for 5.3 Fields (continued)

Field	Data Type	Description	
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.	
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.	

Table B-11 Malware Event Data Block for 5.3 Fields (continued)

Field	Data Type	Description
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
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.

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.

Byte	0 1 2 3			
Bit	0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2			
	Malware Event Block Type (44)			
	Malware Event Block Length			
	Agent UUID			
	Agent UUID, continued			
	Agent UUID, continued			
	Agent UUID, continued			

Byte	0	1	2	3
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1
	Cloud UUID			
	Cloud UUID, continued			
		Cloud UUID), continued	
		Cloud UUID), continued	
		Malware Ever	nt Timestamp	
		Event T	Type ID	
		Event Sul	btype 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 Bloc	k Type (0)	
		String Bloo	ck Length	
		Use	эг	
File Name	String Block Type (0)			
		String Bloo	ck Length	
		File Na	ame	
File Path		String Bloc		
		String Bloo		
	File Path			
File SHA Hash				
		String Bloo		
		File SHA		
		File S		
		File 1		
		File Tim	nestamp	

Byte	0	1	2	3
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 2 3 3 3 4 5 6 7 8 9 0 1
Parent File Name	String Block Type (0)			
Name		String Blo	ock Length	
		Parent Fil	e Name	
Parent File SHA Hash		String Bloo	ck Type (0)	
SIIIII		String Blo	ock Length	
		Parent File S	SHA Hash	
Event Description		String Bloo	ck Type (0)	
		String Blo	ock Length	
		Event Description		
	Device ID			
	Connection Instance Connection Counter		on Counter	
	Connection Event Timestamp			
	Direction Source IP Address			
			ress, continued	
			ress, continued	
		Source IP Add	ress, continued	
	Source IP, cont. Destination IP Address		ss	
			ddress, continued	
	Destination IP Address, continued			
		Destination IP A	ddress, continued	
	Destination IP, cont		Application ID	
	App. ID, cont.		User ID	
	User ID, cont.	Acc	cess Control Policy U	UID

Byte	0	1	2	3
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1
		Access Control Police	cy UUID, continued	
		Access Control Police	cy UUID, continued	
		Access Control Police	cy UUID, continued	
URI	AC Pol UUID, cont.	Disposition	Retro. Disposition	Str. Block Type (0)
	String	g Block Type (0), conti	nued	String Block Length
	Strin	g Block Length, contir	nued	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 Conte	ext, continued	
		Security Conte	ext, continued	
	Security Cont., cont.			

Table B-12 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.

Table B-12 Malware Event Data Block for 5.3.1 Fields (continued)

Field	Data Type	Description	
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.	
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.	

Table B-12 Malware Event Data Block for 5.3.1 Fields (continued)

Field	Data Type	Description
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 3-37 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.
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.

Table B-12 Malware Event Data Block for 5.3.1 Fields (continued)

Field	Data Type	Description
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.
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.

Table B-12 Malware Event Data Block for 5.3.1 Fields (continued)

Field	Data Type	Description								
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								
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.								

Legacy Discovery Data Structures

- Legacy Discovery Event Header, page B-70
- Legacy Server Data Blocks, page B-71
- Legacy Client Application Data Blocks, page B-72
- Legacy Scan Result Data Blocks, page B-74
- Legacy Host Profile Data Blocks, page B-84
- Legacy OS Fingerprint Data Blocks, page B-90

Legacy Discovery Event Header

Discovery Event Header 5.0 - 5.1.1.x

Discovery and connection event messages contain a discovery event header. It conveys the type and subtype of the event, the time the event occurred, the device on which the event occurred, and the structure of the event data in the message. This header is followed by the actual host discovery, user, or connection event data. The structures associated with the different event type/subtype values are described in Host Discovery Structures by Event Type, page 4-36.

The event type and event subtype fields of the discovery event header identify the structure of the transmitted event message. Once the structure of the event data block is determined, your program can parse the message appropriately.

The shaded rows in the following diagram illustrate the format of the discovery event header.

Byte	0	1	2	3										
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1										
	Header V	ersion (1)	Message Type (4)											
		Message	Length											
		Record	l Type											
		Record	Length											
	eStream	ner Server Timestamp (in events, only if bit 2	3 is set)										
	Reser	Reserved for Future Use (in events, only if bit 23 is set)												
Discovery Event Header		Devic	e ID											
	IP Address													
	MAC Address													
	MAC Address, continued Reserved for future use Event Second													
	Reserved (Internal) Event Type													
	Event Subtype													
		File Number (Int	ernal Use Only)											
		File Position (Int	ernal Use Only)											

The following table describes the discovery event header.

Table B-13 Discovery Event Header Fields

Field	Data Types	Description							
Device ID	uint32	ID number of the device that generated the discovery event. You can obtain the metadata for the device by requesting Version 3 and 4 metadata. See Managed Device Record Metadata, page 3-32 for more information.							
IP Address	uint32	IP address of the host involved in the event.							
MAC Address	uint8[6]	MAC address of the host involved in the event.							
Reserved for future use	byte[2]	Two bytes of padding with values set to 0.							
Event Second	uint32	UNIX timestamp (seconds since 01/01/1970) that the system generated the event.							
Event Microsecond	uint32	Microsecond (one millionth of a second) increment that the system generated the event.							
Reserved (Internal)	byte	Internal data from Cisco and can be disregarded.							
Event Type	uint32	Event type (1000 for new events, 1001 for change events, 1002 for user input events, 1050 for full host profile). See Host Discovery Structures by Event Type, page 4-36 for a list of available event types.							
Event Subtype	uint32	Event subtype. See Host Discovery Structures by Event Type, page 4-36 for a list of available event subtypes.							
File Number	byte[4]	Serial file number. This field is for Cisco internal use and can be disregarded.							
File Position	byte[4]	Event's position in the serial file. This field is for Cisco internal use and can be disregarded.							

Legacy Server Data Blocks

For more information, see the following sections:

• Attribute Address Data Block for 5.0 - 5.1.1.x, page B-71

Attribute Address Data Block for 5.0 - 5.1.1.x

The Attribute Address data block contains an attribute list item and is used within an Attribute Definition data block. It has a block type of 38.

The following diagram shows the basic structure of an Attribute Address data block:

By te	0					1							2								3											
Bit	0	1	2	3	4	5	6	7	8	9	1 0	1	1 2	1 3	1 4	1 5	1 6	1 7	1 8	1 9	2 0	2	2 2	2 3	2 4	2 5	2 6	2 7	2 8	2 9	3	3

Attribute Address Block Type (38)
Attribute Address Block Length
Attribute ID
IP Address
Bits

The following table describes the fields of the Attribute Address data block.

Table B-14 Attribute Address Data Block Fields

Field	Data Type	Description
Attribute Address Block Type	uint32	Initiates an Attribute Address data block. This value is always 38.
Attribute Address Block Length	uint32	Number of bytes in the Attribute Address data block, including eight bytes for the attribute address block type and length, plus the number of bytes in the attribute address data that follows.
Attribute ID	uint32	Identification number of the affected attribute, if applicable.
IP Address	uint8[4]	IP address of the host, if the address was automatically assigned, in IP address octets.
Bits	uint32	Contains the significant bits used to calculate the netmask if an IP address was automatically assigned.

Legacy Client Application Data Blocks

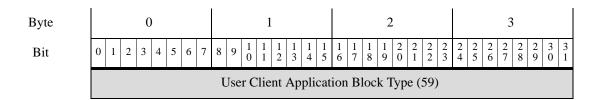
For more information, see the following sections:

• User Client Application Data Block for 5.0 - 5.1, page B-72

User Client Application Data Block for 5.0 - 5.1

The User Client Application data block contains information about the source of the client application data, the identification number for the user who added the data, and the lists of IP address range data blocks. The User Client Application data block has a block type of 59.

The following diagram shows the basic structure of a User Client Application data block:



	User Client Application Block Length
IP Address Ranges	Generic List Block Type (31)
runges	Generic List Block Length
	IP Range Specification Data Blocks*
	Application Protocol ID
	Client Application ID
Version	String Block Type (0)
	String Block Length
	Version

The following table describes the fields of the User Client Application data block.

Table B-15 User Client Application Data Block Fields

Field	Number of Bytes	Description
User Client Application Block Type	uint32	Initiates a User Client Application data block. This value is always 59.
User Client Application Block Length	uint32	Total number of bytes in the User Client Application data block, including eight bytes for the user client application block type and length fields, plus the number of bytes of user client application data that follows.
Generic List Block Type	uint32	Initiates a Generic List data block comprising IP Range Specification data blocks conveying IP address range data. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated IP Range Specification data blocks.
IP Range Specification Data Blocks *	variable	IP Range Specification data blocks containing information about the IP address ranges for the user input. See Table 4-55User Server Data Block Fields, page 4-93 for a description of this data block.
Application Protocol ID	uint32	The internal identification number for the application protocol, if applicable.
Client Application ID	uint32	The internal identification number of the detected client application, if applicable.
String Block Type	uint32	Initiates a String data block that contains the client application version. This value is always 0.
String Block Length	uint32	Number of bytes in the client application version String data block, including the string block type and length fields, plus the number of bytes in the version.
Version	string	Client application version.

Legacy Scan Result Data Blocks

For more information, see the following sections:

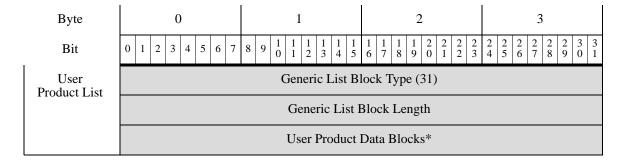
- Scan Result Data Block 5.0 5.1.1.x, page B-74
- User Product Data Block for 5.0.x, page B-76

Scan Result Data Block 5.0 - 5.1.1.x

The Scan Result data block describes a vulnerability and is used within Add Scan Result events (event type 1002, subtype 11). The Scan Result data block has a block type of 102.

The following diagram shows the format of a Scan Result data block:

Byte	0 1	2 3	
Bit	0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 3 3 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1	
	Scan Result Blo	ock Type (102)	
	Scan Result I	Block Length	
	User	r ID	
	Scan	Туре	
	IP Ad	ldress	
	Port	Protocol	
	Flag	Scan Vulnerability	
	List Block Type (11)	List Block Length	List
Vulnerability List	List Block Length	Scan Vulnerability Block Type (109)	
2150	Scan Vulnerability Block Type (109)	Scan Vulnerability Block Length	
	Scan Vulnerability Block Length	Vulnerability Data	
	List Block	Generic Scan Results List	
	List Bloc	Results Elst	
Scan Results List	Generic Scan Result		
2330	Generic Scan Res		
	Generic Sca	nn Results	



The following table describes the fields of the Scan Result data block.

Table B-16 Scan Result Data Block Fields

Field	Data Type	Description	
Scan Result Block Type	uint32	Initiates a Scan Result data block. This value is always 102.	
Scan Result Block Length	uint32	Number of bytes in the Scan Vulnerability data block, including eight bytes for the scan vulnerability block type and length fields, plus the number of bytes of scan vulnerability data that follows.	
User ID	uint32	Contains the user identification number for the user who imported the scan result or ran the scan that produced the scan result.	
Scan Type	uint32	Indicates how the results were added to the system.	
IP Address	uint32	IP address of the host affected by the vulnerabilities in the result, in IP address octets.	
Port	uint16	Port used by the sub-server affected by the vulnerabilities in the results.	
Protocol	uint16	IANA protocol number. For example:	
		• 1 — ICMP	
		• 4 — IP	
		• 6 — TCP	
		• 17 — UDP	
Flag	uint16	Reserved	
List Block Type	uint32	Initiates a List data block comprising Scan Vulnerability data blocks conveying transport Scan Vulnerability data. This value is always 11.	
List Block Length	uint32	Number of bytes in the list. This number includes the eight bytes of the list block type and length fields, plus all encapsulated Scan Vulnerability data blocks.	
		This field is followed by zero or more Scan Vulnerability data blocks.	
Scan Vulnerability Block Type	uint32	Initiates a Scan Vulnerability data block describing a vulnerability detected during a scan. This value is always 109.	
Scan Vulnerability Block Length	uint32	Number of bytes in the Scan Vulnerability data block, including eight bytes for the scan vulnerability block type and length fields, plus the number of bytes in the scan vulnerability data that follows.	

Table B-16 Scan Result Data Block Fields (continued)

Field	Data Type	Description
Vulnerability Data	string	Information relating to each vulnerability.
List Block Type	uint32	Initiates a List data block comprising Scan Vulnerability data blocks conveying transport Scan Vulnerability data. This value is always 11.
List Block Length	uint32	Number of bytes in the list. This number includes the eight bytes of the list block type and length fields, plus all encapsulated Scan Vulnerability data blocks.
		This field is followed by zero or more Scan Vulnerability data blocks.
Generic Scan Results Block Type	uint32	Initiates a Generic Scan Results data block describing server and operating system data detected during a scan. This value is always 108.
Generic Scan Results Block Length	uint32	Number of bytes in the Generic Scan Results data block, including eight bytes for the generic scan results block type and length fields, plus the number of bytes in the scan result data that follows.
Generic Scan Results Data	string	Information relating to each scan result.
Generic List Block Type	uint32	Initiates a Generic List data block comprising User Product data blocks conveying host input data from a third party application. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated User Product data blocks.
User Product Data Blocks *	variable	User Product data blocks containing host input data. See User Product Data Block 5.1+, page 4-155 for a description of this data block.

User Product Data Block for 5.0.x

The User Product data block conveys host input data imported from a third party application, including third party application string mappings. This data block is used in Scan Result Data Block 5.2+, page 4-121. The User Product data block has a block type of 65 for 4.10.x, and a block type of 118 for 5.0 - 5.0.x. The block types have the same structure.



An asterisk(*) next to a data block name in the following diagram indicates that multiple instances of the data block may occur.

The following diagram shows the format of the User Product data block:

Byte	0	1	2	3	
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1	
		User Product Data E	Block Type (65 118)		
		User Product	Block Length		
		Sour	ce ID		
		Source	е Туре		
IP Address Ranges		Generic List B	lock Type (31)		
		Generic List	Block Length		
		IP Range Specifica	ation Data Blocks*		
	Po	ort	Prot	tocol	
		Drop Use	r Product		
Custom Vendor String		String Bloo	ck Type (0)		
	String Block Length				
	Custom Vendor String				
Custom Product String	String Block Type (0)				
	String Block Length				
Custom Product String			duct String		
Custom Version String Block Type (0)		ck Type (0)			
	String Block Length				
	Custom Version String				
		Softw	are ID		
Server ID Vendor ID					
	Product ID				
Major Version String		String Bloo	ck Type (0)		
	String Block Length				
	Major Version String				

Byte	0	1	2	3
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 3 3 4 5 6 7 8 9 0 1
Minor Version	String Block Type (0)			
String		String Blo	ck Length	
		Minor Vers	ion String	
Revision String		String Bloo	ck Type (0)	
String		String Blo	ck Length	
		Revision	String	
To Major String		String Bloo	ck Type (0)	
String		String Blo	ck Length	
		To Major Ver	rsion String	
To Minor String		String Bloo	ck Type (0)	
String		String Blo	ck Length	
		To Minor Ver	rsion String	
To Revision String		String Bloo	ck Type (0)	
2 111128		String Blo	ck Length	
		To Revision	on String	
Build String		String Bloo	ck Type (0)	
		String Blo	ck Length	
		Build S	String	
Patch String		String Bloo	ck Type (0)	
	String Block Length			
		Patch S	String	
Extension String		String Bloo	ck Type (0)	
6		String Blo	ck Length	
		Extension	n String	

Byte	0	1	2	3
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1
OS UUID		Operating Sy	stem UUID	
		Operating Syste	em UUID cont.	
		Operating Syste	em UUID cont.	
		Operating Syste	em UUID cont.	
List of Fixes		Generic List Blo	ock Type (31)	
		Generic List B	Block Length	
		Fix List Dat	ta Blocks*	

The following table describes the components of the User Product data block.

Table B-17 User Product Data Block Fields for 4.10.x, 5.0-5.0.x

Field	Data Type	Description		
User Product Data Block Type	uint32	Initiates a User Product data block. This value is 65 for version 4.10.x and 118 for version 5.0 - 5.0.x.		
User Product Block Length	uint32	Total number of bytes in the User Product data block, including eight bytes for the user product block type and length fields, plus the number of bytes in the user product data that follows.		
Source ID	uint32	Identification number of the source that imported the data.		
Source Type	uint32	The source type of the source that supplied the data.		
Generic List Block Type	uint32	Initiates a Generic List data block comprising IP Range Specification data blocks conveying IP address range data. This value is always 31.		
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated IP Range Specification data blocks.		
IP Range Specification Data Blocks *	variable	IP Range Specification data blocks containing information about the IP address ranges for the user input. See IP Address Range Data Block for 5.2+, page 4-86 for a description of this data block.		
Port	uint16	Port specified by the user.		
Protocol	uint16	IANA protocol number specified by the user. For example: • 1 — ICMP • 4 — IP • 6 — TCP • 17 — UDP		
Drop User Product	uint32	Indicates whether the user OS definition was deleted from the host: • 0 — No • 1 — Yes		

Table B-17 User Product Data Block Fields for 4.10.x, 5.0-5.0.x (continued)

Field	Data Type	Description	
String Block Type	uint32	Initiates a String data block containing the custom vendor name specified in the user input. This value is always 0.	
String Block Length	uint32	Number of bytes in the custom vendor String data block, including eight bytes for the block type and length fields, plus the number of bytes in the vendor name.	
Custom Vendor Name	string	The custom vendor name specified in the user input.	
String Block Type	uint32	Initiates a String data block containing the custom product name specified in the user input. This value is always 0.	
String Block Length	uint32	Number of bytes in the custom product String data block, including eight bytes for the block type and length fields, plus the number of bytes in the product name.	
Custom Product Name	string	The custom product name specified in the user input.	
String Block Type	uint32	Initiates a String data block containing the custom version specified in the user input. This value is always 0.	
String Block Length	uint32	Number of bytes in the custom version String data block, including eight bytes for the block type and length fields, plus the number of bytes in the version.	
Custom Version	string	The custom version specified in the user input.	
Software ID	uint32	The identifier for a specific revision of a server or operating system in the Cisco database.	
Server ID	uint32	The Cisco application identifier for the application protocol on the host server specified in user input.	
Vendor ID	uint32	The identifier for the vendor of a third party operating system specified when the third party operating system is mapped to a Cisco 3D operating system definition.	
Product ID	uint32	The product identification string of a third party operating system string specified when the third party operating system string is mapped to a Cisco 3D operating system definition.	
String Block Type	uint32	Initiates a String data block containing the major version number of the Cisco 3D operating system definition that a third party operating system string in the user input is mapped to. This value is always 0.	
String Block Length	uint32	Number of bytes in the major String data block, including eight bytes for the block type and length fields, plus the number of bytes in the version.	
Major Version	string	Major version of the Cisco 3D operating system definition that a third party operating system string is mapped to.	
String Block Type	uint32	Initiates a String data block containing the minor version number of the Cisco 3D operating system definition that a third party operating system string is mapped to. This value is always 0.	

Table B-17 User Product Data Block Fields for 4.10.x, 5.0-5.0.x (continued)

Field	Data Type	Description
String Block Length	uint32	Number of bytes in the minor String data block, including eight bytes for the block type and length fields, plus the number of bytes in the version.
Minor Version	string	Minor version number of the Cisco 3D operating system definition that a third party operating system string in the user input is mapped to.
String Block Type	uint32	Initiates a String data block containing the revision number of the Cisco operating system definition that a third party operating system string in the user input is mapped to. This value is always 0.
String Block Length	uint32	Number of bytes in the revision String data block, including eight bytes for the block type and length fields, plus the number of bytes in the revision number.
Revision	string	Revision number of the Cisco 3D operating system definition that a third party operating system string in the user input is mapped to.
String Block Type	uint32	Initiates a String data block containing the last major version of the Cisco 3D operating system definition that a third party operating system string is mapped to. This value is always 0.
String Block Length	uint32	Number of bytes in the To Major String data block, including eight bytes for the block type and length fields, plus the number of bytes in the version.
To Major	string	Last version number in a range of major version numbers of the Cisco 3D operating system definition that a third party operating system string in the user input is mapped to.
String Block Type	uint32	Initiates a String data block containing the last minor version of the Cisco 3D operating system definition that a third party operating system string is mapped to. This value is always 0.
String Block Length	uint32	Number of bytes in the To Minor String data block, including eight bytes for the block type and length fields, plus the number of bytes in the version.
To Minor	string	Last version number in a range of minor version numbers of the Cisco 3D operating system definition that a third party operating system string in the user input is mapped to.
String Block Type	uint32	Initiates a String data block containing the Last revision number of the Cisco 3D operating system definition that a third party operating system string is mapped to. This value is always 0.
String Block Length	uint32	Number of bytes in the To Revision String data block, including eight bytes for the block type and length fields, plus the number of bytes in the revision number.
To Revision	string	Last revision number in a range of revision numbers of the Cisco 3D operating system definitions that a third party operating system string in the user input is mapped to.
String Block Type	uint32	Initiates a String data block containing the build number of the Cisco 3D operating system that the third party operating system string is mapped. This value is always 0.

Table B-17 User Product Data Block Fields for 4.10.x, 5.0-5.0.x (continued)

Field	Data Type	Description
String Block Length	uint32	Number of bytes in the build String data block, including eight bytes for the block type and length fields, plus the number of bytes in the build number.
Build	string	Build number of the Cisco 3D operating system that the third party operating system string in the user input is mapped to.
String Block Type	uint32	Initiates a String data block containing the patch number of the Cisco 3D operating system that the third party operating system string is mapped to. This value is always 0.
String Block Length	uint32	Number of bytes in the patch String data block, including eight bytes for the block type and length fields, plus the number of bytes in the patch number.
Patch	string	Patch number of the Cisco 3D operating system that the third party operating system string in the user input is mapped to.
String Block Type	uint32	Initiates a String data block containing the extension number of the Cisco 3D operating system that the third party operating system string is mapped. This value is always 0.
String Block Length	uint32	Number of bytes in the extension String data block, including eight bytes for the block type and length fields, plus the number of bytes in the extension number.
Extension	string	Extension number of the Cisco 3D operating system that the third party operating system string in the user input is mapped to.
UUID	uint8 [x16]	Contains the unique identification number for the operating system.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Fix List data blocks conveying user input data regarding what fixes have been applied to hosts in the specified IP address ranges. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Fix List data blocks.
Fix List Data Blocks *	variable	Fix List data blocks containing information about fixes applied to the hosts. See Fix List Data Block, page 4-92 for a description of this data block.

Legacy User Login Data Blocks

See the following sections for more information:

• User Login Information Data Block for 5.0 - 5.0.2, page B-82

User Login Information Data Block for 5.0 - 5.0.2

The User Login Information data block is used in User Information Update messages and conveys changes in login information for a detected user. For more information, see User Information Update Message Block, page 4-54.

The User Login Information data block has a block type of 121 for version 5.0 - 5.0.2.

The graphic below shows the format of the User Login Information data block:

Byte	0	1	2	3
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1
	User Login Information Block Type (121)			
	User Login Information Block Length			
		Times	stamp	
		IP Address		
User Name	String Block Type (0)			
1 (1111)	String Block Length			
	User Name			
	User ID			
		Applica	tion ID	
Email	String Block Type (0)			
	String Block Length			
	Email			

The following table describes the components of the User Login Information data block.

Table B-18 User Login Information Data Block Fields 5.0 - 5.0.2

Field	Data Type	Description
User Login Information Block Type	uint32	Initiates a User Login Information data block. This value is 121 for version 5.0 - 5.0.2.
User Login Information Block Length	uint32	Total number of bytes in the User Login Information data block, including eight bytes for the user login information block type and length fields, plus the number of bytes in the user login information data that follows.
Timestamp	uint32	Timestamp of the event.
IP Address	uint8[4]	IP address from the host where the user was detected logging in, in IP address octets.
String Block Type	uint32	Initiates a String data block containing the username for the user. This value is always 0.
String Block Length	uint32	Number of bytes in the username String data block, including eight bytes for the block type and length fields, plus the number of bytes in the username.

lable B-18	User Login Information Data Block Fields 5.0 - 5.0.2 (continued)

Field	Data Type	Description
Username	string	The user name for the user.
User ID	uint32	Identification number of the user.
Application ID	uint32	The application ID for the application protocol used in the connection that the login information was derived from.
String Block Type	uint32	Initiates a String data block containing the email address for the user. This value is always 0.
String Block Length	uint32	Number of bytes in the email address String data block, including eight bytes for the block type and length fields, plus the number of bytes in the email address.
Email	string	The email address for the user.

Legacy Host Profile Data Blocks

See the following sections for more information:

• Host Profile Data Block for 5.0 - 5.0.2, page B-84

Host Profile Data Block for 5.0 - 5.0.2

The following diagram shows the format of a Host Profile data block in versions 5.0 to 5.0.2. The Host Profile data block also does not include a host criticality value, but does include a VLAN presence indicator. In addition, a Host Profile data block can convey a NetBIOS name for the host. This Host Profile data block has a block type of 91.



An asterisk(*) next to a block type field in the following diagram indicates the message may contain zero or more instances of the series 1 data block.

Byte	0	1	2	3	
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 3 3 4 5 6 7 8 9 0 1	
	Host Profile Block Type (91)				
	Host Profile Block Length				
	IP Address				
Server Fingerprints	Hops	Primary/Secondary	Generic List B	lock Type (31)	
1 ingerprints	Generic List Block Type, continued Generic List Block Length			Block Length	
	Generic List Block Length, continued		Server Fingerpri	int Data Blocks*	

Byte	0 1 2 3				
Bit	0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2				
Client Fingerprints	Generic List Block Type (31)				
ringerprints	Generic List Block Length				
	Client Fingerprint Data Blocks*				
SMB Fingerprints	Generic List Block Type (31)				
1 mgcrprmts	Generic List Block Length				
	SMB Fingerprint Data Blocks*				
DHCP Fingerprints	Generic List Block Type (31)				
1 mgerprints	Generic List Block Length				
	DHCP Fingerprint Data Blocks*				
	List Block Type (11)	List of TCP Servers			
	List Block Length				
TCP Server Block*	Server Block Type (36)				
	Server Block Length				
	TCP Server Data				
	List Block Type (11)	List of UDP Servers			
	List Block Length	200,000			
UDP Server Block*	Server Block Type (36)*				
210411	Server Block Length				
	UDP Server Data				
	List Block Type (11)	List of Network			
	List Block Length	Protocols			
Network Protocol	Protocol Block Type (4)*				
Block*	Protocol Block Length				
	Network Protocol Data				

Byte	0	1	2	3	
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1	
		List Block Type (11)			List of Transport
		List Bloc	k Length		Protocols
Transport Protocol		Protocol Blo	ck Type (4)*		
Block*		Protocol Bl	ock Length		
		Transport Pro	otocol Data		
		List Block	Type (11)		List of MAC Addresses
		List Bloc	k Length		1100105505
MAC Address Block*		MAC Address E	Block Type (95)*		
		MAC Address	Block Length		
	MAC Address Data				
	Host Last Seen				
	Host Type				
	VLAN Presence	VLA	N ID	VLAN Type	
	VLAN Priority Generic List Block Type (31)				List of Client Applications
	Generic List Block Type, continued Generic List Block Length		rr ·····		
Client App Data	Generic List Block Length, continued Client Application Block Type (112)*				
	Client App Block Type (29)*, con't	Clier	nt Application Block Le	ength	
	Client Application Block Length, con't	C	lient Application Data		
NetBIOS Name		String Bloo	ck Type (0)		
	String Block Length				
	NetBIOS String Data				

The following table describes the fields of the host profile data block returned by version 4.9 to version 5.0.2.

Table B-19 Host Profile Data Block for 5.0 - 5.0.2 Fields

Field	Data Type	Description
Host Profile Block Type	uint32	Initiates the Host Profile data block for 4.9 to 5.0.2. This data block has a block type of 91.
Host Profile Block Length	uint32	Number of bytes in the Host Profile data block, including eight bytes for the host profile block type and length fields, plus the number of bytes included in the host profile data that follows.
IP Address	uint8[4]	IP address of the host described in the profile, in IP address octets.
Hops	uint8	Number of hops from the host to the device.
Primary/ Secondary	uint8	Indicates whether the host is in the primary or secondary network of the device that detected it:
		• 0 — Host is in the primary network.
		• 1 — Host is in the secondary network.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data identified using a server fingerprint. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.
Operating System Fingerprint (Server Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host identified using a server fingerprint. See Operating System Fingerprint Data Block for 5.0 - 5.0.2, page B-91 for a description of this data block.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data identified using a client fingerprint. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.
Operating System Fingerprint (Client Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host identified using a client fingerprint. See Operating System Fingerprint Data Block for 5.0 - 5.0.2, page B-91 for a description of this data block.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data identified using an SMB fingerprint. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.

Table B-19 Host Profile Data Block for 5.0 - 5.0.2 Fields (continued)

Field	Data Type	Description
Operating System Fingerprint (SMB Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host identified using an SMB fingerprint. See Operating System Fingerprint Data Block for 5.0 - 5.0.2, page B-91 for a description of this data block.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data identified using a DHCP fingerprint. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.
Operating System Fingerprint (DHCP Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host identified using a DHCP fingerprint. See Operating System Fingerprint Data Block for 5.0 - 5.0.2, page B-91 for a description of this data block.
List Block Type	uint32	Initiates a List data block comprising Server data blocks conveying TCP server data. This value is always 11.
List Block Length	uint32	Number of bytes in the list. This number includes the eight bytes of the list block type and length fields, plus all encapsulated Server data blocks.
		This field is followed by zero or more Server data blocks.
Server Block Type	uint32	Initiates a Server data block. This value is always 89.
Server Block Length	uint32	Number of bytes in the Server data block, including eight bytes for the server block type and length fields, plus the number of bytes of TCP server data that follows.
TCP Server Data	variable	Data fields describing a TCP server (as documented for earlier versions of the product).
List Block Type	uint32	Initiates a List data block comprising Server data blocks conveying UDP server data. This value is always 11.
List Block Length	uint32	Number of bytes in the list. This number includes the eight bytes of the list block type and length fields, plus all encapsulated Server data blocks.
		This field is followed by zero or more Server data blocks.
Server Block Type	uint32	Initiates a Server data block describing a UDP server. This value is always 89.
Server Block Length	uint32	Number of bytes in the Server data block, including eight bytes for the server block type and length fields, plus the number of bytes of UDP server data that follows.
UDP Server Data	variable	Data fields describing a UDP server (as documented for earlier versions of the product).

Table B-19 Host Profile Data Block for 5.0 - 5.0.2 Fields (continued)

Field	Data Type	Description
List Block Type	uint32	Initiates a List data block comprising Protocol data blocks conveying network protocol data. This value is always 11.
List Block Length	uint32	Number of bytes in the list. This number includes the eight bytes of the list block type and length fields, plus all encapsulated Protocol data blocks.
		This field is followed by zero or more Protocol data blocks.
Protocol Block Type	uint32	Initiates a Protocol data block describing a network protocol. This value is always 4.
Protocol Block Length	uint32	Number of bytes in the Protocol data block, including eight bytes for the protocol block type and length fields, plus the number of bytes in the protocol data that follows.
Network Protocol Data	uint16	Data field containing a network protocol number, as documented in Protocol Data Block, page 4-67.
List Block Type	uint32	Initiates a List data block comprising Protocol data blocks conveying transport protocol data. This value is always 11.
List Block Length	uint32	Number of bytes in the list. This number includes the eight bytes of the list block type and length fields, plus all encapsulated Protocol data blocks.
		This field is followed by zero or more transport protocol data blocks.
Protocol Block Type	uint32	Initiates a Protocol data block describing a transport protocol. This value is always 4.
Protocol Block Length	uint32	Number of bytes in the protocol data block, including eight bytes for the protocol block type and length, plus the number of bytes in the protocol data that follows.
Transport Protocol Data	variable	Data field containing a transport protocol number, as documented in Protocol Data Block, page 4-67.
List Block Type	uint32	Initiates a List data block comprising MAC Address data blocks. This value is always 11.
List Block Length	uint32	Number of bytes in the list, including the list header and all encapsulated MAC Address data blocks.
Host MAC Address Block Type	uint32	Initiates a Host MAC Address data block. This value is always 95.
Host MAC Address Block Length	uint32	Number of bytes in the Host MAC Address data block, including eight bytes for the Host MAC address block type and length fields, plus the number of bytes in the Host MAC address data that follows.
Host MAC Address Data	variable	Host MAC address data fields described in Host MAC Address 4.9+, page 4-105.
Host Last Seen	uint32	UNIX timestamp that represents the last time the system detected host activity.

Table B-19 Host Profile Data Block for 5.0 - 5.0.2 Fields (continued)

Field	Data Type	Description
Host Type	uint32	Indicates the host type. The following values may appear:
		• 0 — Host
		• 1 — Router
		• 2 — Bridge
		• 3 — NAT device
		• 4 — LB (load balancer)
VLAN Presence	uint8	Indicates whether a VLAN is present:
		• 0 — Yes
		• 1 — No
VLAN ID	uint16	VLAN identification number that indicates which VLAN the host is a member of.
VLAN Type	uint8	Type of packet encapsulated in the VLAN tag.
VLAN Priority	uint8	Priority value included in the VLAN tag.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Client Application data blocks conveying client application data. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated client application data blocks.
Client Application Block Type	uint32	Initiates a client application block. This value is always 5.
Client Application Block Length	uint32	Number of bytes in the client application block, including eight bytes for the client application block type and length fields, plus the number of bytes in the client application data that follows.
Client Application Data	variable	Client application data fields describing a client application, as documented in Host Client Application Data Block for 5.0+, page 4-140.
String Block Type	uint32	Initiates a string data block for the NetBIOS name. This value is set to 0 to indicate string data.
String Block Length	uint32	Indicates the number of bytes in the NetBIOS name data block, including eight bytes for the string block type and length, plus the number of bytes in the NetBIOS name.
NetBIOS String Data	Variable	Contains the NetBIOS name of the host described in the host profile.

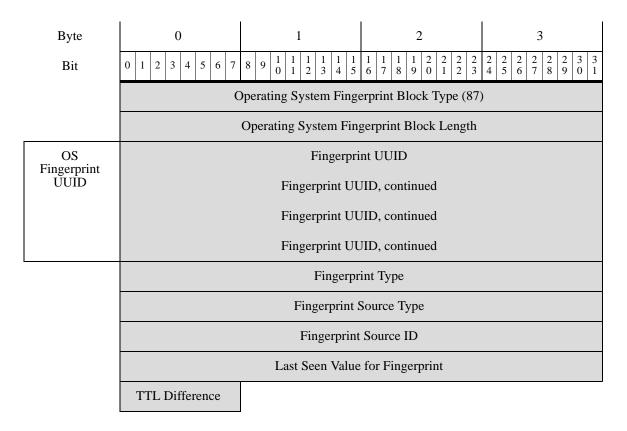
Legacy OS Fingerprint Data Blocks

See the following sections for more information:

• Operating System Fingerprint Data Block for 5.0 - 5.0.2, page B-91

Operating System Fingerprint Data Block for 5.0 - 5.0.2

The Operating System Fingerprint data block has a block type of 87. The block includes a fingerprint Universally Unique Identifier (UUID), as well as the fingerprint type, the fingerprint source type, and the fingerprint source ID. The following diagram shows the format of an Operating System Fingerprint data block for version 5.0 to version 5.0.2.



The following table describes the fields of the operating system fingerprint data block.

Table B-20 Operating System Fingerprint Data Block Fields

Field	Data Type	Description
Operating System Fingerprint Data Block Type	uint32	Initiates the operating system data block. This value is always 87.
Operating System Data Block Length	uint32	Number of bytes in the Operating System Fingerprint data block. This value should always be 41: eight bytes for the data block type and length fields, sixteen bytes for the fingerprint UUID value, four bytes for the fingerprint type, four bytes for the fingerprint source type, four bytes for the fingerprint source ID, four bytes for the last seen value, and one byte for the TTL difference.

Table B-20 Operating System Fingerprint Data Block Fields (continued)

Field	Data Type	Description
Fingerprint UUID	uint8[16]	Fingerprint identification number, in octets, that acts as a unique identifier for the operating system. The fingerprint UUID maps to the operating system name, vendor, and version in the vulnerability database (VDB).
Fingerprint Type	uint32	Indicates the type of fingerprint.
Fingerprint Source Type	uint32	Indicates the type (i.e., user or scanner) of the source that supplied the operating system fingerprint.
Fingerprint Source ID	uint32	Indicates the ID of the source that supplied the operating system fingerprint.
Last Seen	uint32	Indicates when the fingerprint was last seen in traffic.
TTL Difference	uint8	Indicates the difference between the TTL value in the fingerprint and the TTL value seen in the packet used to fingerprint the host.

Legacy Connection Data Structures

For more information, see the following sections:

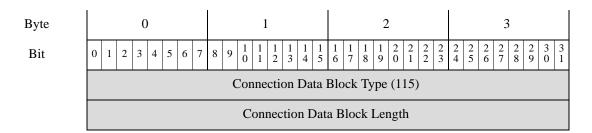
- Connection Statistics Data Block 5.0 5.0.2, page B-92
- Connection Statistics Data Block 5.1, page B-97
- Connection Statistics Data Block 5.2.x, page B-103
- Connection Chunk Data Block for 5.0 5.1, page B-108
- Connection Statistics Data Block 5.1.1.x, page B-110
- Connection Statistics Data Block 5.3, page B-116
- Connection Statistics Data Block 5.3.1, page B-123

Connection Statistics Data Block 5.0 - 5.0.2

The Connection Statistics data block is used in Connection Data messages. The Connection Statistics data block for version 5.0 - 5.0.2 has a block type of 115.

For more information on the Connection Statistics Data message, see Connection Statistics Data Message, page 4-45.

The following diagram shows the format of a Connection Statistics data block for 5.0 - 5.0.2:



FireSIGHT eStreamer Integration Guide

Byte	0 1 2 3							
Bit	0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1							
	Device ID							
	Ingress Zone							
	Ingress Zone, continued							
	Ingress Zone, continued							
	Ingress Zone, continued							
	Egress Zone							
	Egress Zone, continued							
	Egress Zone, continued							
	Egress Zone, continued							
	Ingress Interface							
	Ingress Interface, continued							
	Ingress Interface, continued							
	Ingress Interface, continued							
	Egress Interface							
	Egress Interface, continued							
	Egress Interface, continued							
	Egress Interface, continued							
	Initiator IP Address							
	Initiator IP Address, continued							
	Initiator IP Address, continued							
	Initiator IP Address, continued							
	Responder IP Address							
	Responder IP Address, continued							
	Responder IP Address, continued							
	Responder IP Address, continued							
	Policy Revision							

Byte

Bit

0 1	0 1 2			
0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 5	1 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1		
Policy Revision	on, continued			
Policy Revision	on, continued			
Policy Revision	on, continued			
Rule	ID			
Rule A	action			
Initiator Port	Respond	ler Port		
TCP Flags	Protocol	NetFlow Source		
NetFlow Sour	ce, continued			
NetFlow Sour	ce, continued			
NetFlow Sour	ce, continued			
NetFlow Source, continue	ed	First Pkt Time		
First Packet Timestamp, cont	inued	Last Pkt Time		
Last Packet Timestamp, cont	Packets Sent			
Packets Sent, continued				
Packets Sent, continued		Packets Rcvd		
Packets Receiv				
Packets Received, continu	Bytes Sent			
Bytes Sent,				
Packets Received, continu	Bytes Rcvd			
Bytes Received, continued				
Bytes Received, continue	User ID			
User ID, continued		Application Protocol ID		
Application Protocol ID, con	inued	URL Category		
URL Category, continue	d	URL Reputation		
URL Reputation, continu	ed	Client App ID		

Byte	0	1	2	3			
Bit	0 1 2 3 4 5 6 7 8	9 1 1 1 1 1 1 1 5	1 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1			
	Client A	Application ID, contin	nued	Web App ID			
	Web A	pplication ID, contin	ued	String Block Type (0)			
Client App URL	String	Block Type, continu	ied	String Block Length			
	String 1	Client Application URL					
NetBIOS Name	String Block Type (0)						
Tunie	String Block Length						
	NetBIOS Name						
Client App Version	String Block Type (0)						
Tipp (croion	String Block Length						
		Client Applicat	tion Version				

The following table describes the fields of the Connection Statistics data block for 5.0 - 5.0.2.

Table B-21 Connection Statistics Data Block 5.0 - 5.0.2 Fields

Field	Data Type	Description
Connection Statistics Data Block Type	uint32	Initiates a Connection Statistics data block for 5.0 to 5.0.2. The value is always 115.
Connection Statistics Data Block Length	uint32	Number of bytes in the Connection Statistics data block, including eight bytes for the connection statistics block type and length fields, plus the number of bytes in the connection data that follows.
Device ID	uint32	The device that detected the connection event.
Ingress Zone	uint8[16]	Ingress security zone in the event that triggered the policy violation.
Egress Zone	uint8[16]	Egress security zone in the event that triggered the policy violation.
Ingress Interface	uint8[16]	Interface for the inbound traffic.
Egress Interface	uint8[16]	Interface for the outbound traffic.
Initiator IP Address	uint8[16]	IP address of the host that initiated the session described in the connection event, in IP address octets.
Responder IP Address	uint8[16]	IP address of the host that responded to the initiating host, in IP address octets.
Policy Revision	uint8[16]	Revision number of the rule associated with the triggered correlation event, if applicable.

Table B-21 Connection Statistics Data Block 5.0 - 5.0.2 Fields (continued)

Field	Data Type	Description
Rule ID	uint32	Internal identifier for the rule that triggered the event, if applicable.
Rule Action	uint32	The action selected in the user interface for that rule (allow, block, and so forth).
Initiator Port	uint16	Port used by the initiating host.
Responder Port	uint16	Port used by the responding host.
TCP Flags	uint16	Indicates any TCP flags for the connection event.
Protocol	uint8	The IANA-specified protocol number.
NetFlow Source	uint8[16]	IP address of the NetFlow-enabled device that exported the data for the connection
First Packet Timestamp	uint32	UNIX timestamp of the date and time the first packet was exchanged in the session.
Last Packet Timestamp	uint32	UNIX timestamp of the date and time the last packet was exchanged in the session.
Packets Sent	uint64	Number of packets transmitted by the initiating host.
Packets Received	uint64	Number of packets transmitted by the responding host.
Bytes Sent	uint64	Number of bytes transmitted by the initiating host.
Bytes Received	uint64	Number of bytes transmitted by the responding host.
User ID	uint32	Internal identification number for the user who last logged into the host that generated the traffic.
Application Protocol ID	uint32	Application ID of the application protocol.
URL Category	uint32	The internal identification number of the URL category.
URL Reputation	uint32	The internal identification number for the URL reputation.
Client Application ID	uint32	The internal identification number of the detected client application, if applicable.
Web Application ID	uint32	The internal identification number of the detected web application, if applicable.
String Block Type	uint32	Initiates a String data block for the client application URL. This value is always 0.
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 client application URL string.
Client Application URL	string	URL the client application accessed, if applicable (/files/index.html, for example).
String Block Type	uint32	Initiates a String data block for the host NetBIOS name. This value is always 0.
String Block Length	uint32	Number of bytes in the String data block, including eight bytes for the string block type and length fields, plus the number of bytes in the NetBIOS name string.

Table B-21 Connection Statistics Data Block 5.0 - 5.0.2 Fields (continued)

Field	Data Type	Description			
NetBIOS Name	string	Host NetBIOS name string.			
String Block Type	uint32	Initiates a String data block for the client application version. This value is always 0.			
String Block Length	uint32	Number of bytes in the String data block for the client application version, including eight bytes for the string block type and length, plus the number of bytes in the version.			
Client Application Version	string	Client application version.			

Connection Statistics Data Block 5.1

The Connection Statistics data block is used in Connection Data messages. Changes to the Connection data block between 5.0.2 and 5.1 include the addition of new fields with configuration parameters introduced in 5.1 (rule action reason, monitor rules, Security Intelligence source/destination, Security Intelligence layer). The Connection Statistics data block for version 5.1 has a block type of 126.

For more information on the Connection Statistics Data message, see Connection Statistics Data Message, page 4-45.

The following diagram shows the format of a Connection Statistics data block for 5.1:

0 3 Byte 2 1 1 7 Bit 3 Connection Data Block Type (126) Connection Data Block Length Device ID Ingress Zone Ingress Zone, continued Ingress Zone, continued Ingress Zone, continued Egress Zone Egress Zone, continued Egress Zone, continued Egress Zone, continued

Byte	0		1			2						3			
Bit	0 1 2 3 4 5 6 7 8 9 1 1 1 1 3					1 6	1 1 7 8	1 2 9 0	2	2 2	2 2 4	2 2 5 6	2 7	2 8 9	3 3 0 1
	Ingress Interface														
			Ingre	ss Int	erfa	ice,	cont	inued							
			Ingre	ss Int	erfa	ice,	cont	inued							
			Ingre	ss Int				inued							
				Egre											
			_	ss Inte											
			_	ss Inte											
				ss Inte											
		T		nitiato											
				or IP A											
				or IP											
	Initiator IP Address, continued														
	Responder IP Address Responder IP Address, continued														
	Responder IP Address, continued														
	Responder IP Address, continued														
	Policy Revision														
			Polic	y Rev	isi	on,	conti	nued							
			Polic	y Rev	isi	on,	conti	nued							
			Polic	y Rev	isi	on,	conti	nued							
	Rule ID														
	Rule Action Rule Reason														
	Initiato	or Port							Re	espo	ndei	r Port			
	TCP	Flags					P	rotoco	ol			NetF	low	Sou	rce
			NetF	low S	our	ce,	conti	nued							
			NetF	low S	our	ce,	conti	nued							

Byte	0	1	2	3			
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5 NetFlow Sour		2 2 2 2 2 3 3 3 4 5 6 7 8 9 0 1			
	Ne	etFlow Source, continu	ed	First Pkt Time			
	First P	Packet Timestamp, con	tinued	Last Pkt Time			
	Last P	Packet Timestamp, con	tinued	Initiator Transmitted Packets			
		Initiator Transmitted	l Packets, continued				
	Initiator '	Transmitted Packets, c	ontinued	Responder Transmitted Packets			
		Responder Transmitte	ed Packets, continued				
	Responder	r Transmitted Packets,	continued	Initiator Transmitted Bytes			
	Initiator Transmitted Bytes, continued						
	Initiator	Responder Transmitted Bytes					
	Responder Transmitted Bytes, continued						
	Responde	User ID					
		User ID, continued		Application Protocol ID			
	Applic	cation Protocol ID, con	tinued	URL Category			
	U	RL Category, continue	ed	URL Reputation			
	UF	RL Reputation, continu	ed	Client App ID			
	Clien	t Application ID, cont	nued	Web App ID			
	Web	String Block Type (0)					
Client App URL	Stri	ng Block Type, contin	ued	String Block Length			
	Strin	g Block Length, conti	nued	Client Application URL			

Byte	0	1	2	3				
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1				
NetBIOS Name		String Bloc	k Type (0)					
Tunic		String Bloo	ck Length					
		NetBIOS	Name					
Client App Version		String Bloc	k Type (0)					
ripp version		String Bloo	ck Length					
		Client Applica	tion Version					
		Monitor Rule 1						
	Monitor Rule 2							
	Monitor Rule 3							
	Monitor Rule 4							
	Monitor Rule 5							
	Monitor Rule 6							
	Monitor Rule 7							
	Monitor Rule 8							
	Sec. Int. Src/Dst	Sec. Int. Rep Layer						

The following table describes the fields of the Connection Statistics data block for 5.1.

Table B-22 Connection Statistics Data Block 5.1 Fields

Field	Data Type	Description
Connection Statistics Data Block Type	uint32	Initiates a Connection Statistics data block for 5.1. The value is always 126.
Connection Statistics Data Block Length	uint32	Number of bytes in the Connection Statistics data block, including eight bytes for the connection statistics block type and length fields, plus the number of bytes in the connection data that follows.
Device ID	uint32	The device that detected the connection event.
Ingress Zone	uint8[16]	Ingress security zone in the event that triggered the policy violation.
Egress Zone	uint8[16]	Egress security zone in the event that triggered the policy violation.
Ingress Interface	uint8[16]	Interface for the inbound traffic.
Egress Interface	uint8[16]	Interface for the outbound traffic.

Table B-22 Connection Statistics Data Block 5.1 Fields (continued)

Field	Data Type	Description			
Initiator IP Address	uint8[16]	IP address of the host that initiated the session described in the connection event, in IP address octets.			
Responder IP Address	uint8[16]	IP address of the host that responded to the initiating host, in IP address octets.			
Policy Revision	uint8[16]	Revision number of the rule associated with the triggered correlation event, if applicable.			
Rule ID	uint32	Internal identifier for the rule that triggered the event, if applicable.			
Rule Action	uint16	The action selected in the user interface for that rule (allow, block, and so forth).			
Rule Reason	uint16	The reason the rule triggered the event.			
Initiator Port	uint16	Port used by the initiating host.			
Responder Port	uint16	Port used by the responding host.			
TCP Flags	uint16	Indicates any TCP flags for the connection event.			
Protocol	uint8	The IANA-specified protocol number.			
NetFlow Source	uint8[16]	IP address of the NetFlow-enabled device that exported the data for the connection.			
First Packet Timestamp	uint32	UNIX timestamp of the date and time the first packet was exchanged in the session.			
Last Packet Timestamp	uint32	UNIX timestamp of the date and time the last packet was exchanged in the session.			
Initiator Transmitted Packets	uint64	Number of packets transmitted by the initiating host.			
Responder Transmitted Packets	uint64	Number of packets transmitted by the responding host.			
Initiator Transmitted Bytes	uint64	Number of bytes transmitted by the initiating host.			
Responder Transmitted Bytes	uint64	Number of bytes transmitted by the responding host.			
User ID	uint32	Internal identification number for the user who last logged into the host that generated the traffic.			
Application Protocol ID	uint32	Application ID of the application protocol.			
URL Category	uint32	The internal identification number of the URL category.			
URL Reputation	uint32	The internal identification number for the URL reputation.			
Client Application ID	uint32	The internal identification number of the detected client application, if applicable.			
Web Application ID	uint32	The internal identification number of the detected web application, if applicable.			

Table B-22 Connection Statistics Data Block 5.1 Fields (continued)

Field	Data Type	Description	
String Block Type	uint32	Initiates a String data block for the client application URL. This value is always 0.	
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 client application URL string.	
Client Application URL	string	URL the client application accessed, if applicable (/files/index.html, for example).	
String Block Type	uint32	Initiates a String data block for the host NetBIOS name. This value is always 0.	
String Block Length	uint32	Number of bytes in the String data block, including eight bytes for the string block type and length fields, plus the number of bytes in the NetBIOS name string.	
NetBIOS Name	string	Host NetBIOS name string.	
String Block Type	uint32	Initiates a String data block for the client application version. This value is always 0.	
String Block Length	uint32	Number of bytes in the String data block for the client application version, including eight bytes for the string block type and length, plus the number of bytes in the version.	
Client Application Version	string	Client application version.	
Monitor Rule 1	uint32	The ID of the first monitor rule associated with the connection event.	
Monitor Rule 2	uint32	The ID of the second monitor rule associated with the connection event.	
Monitor Rule 3	uint32	The ID of the third monitor rule associated with the connection event.	
Monitor Rule 4	uint32	The ID of the fourth monitor rule associated with the connection event.	
Monitor Rule 5	uint32	The ID of the fifth monitor rule associated with the connection event.	
Monitor Rule 6	uint32	The ID of the sixth monitor rule associated with the connection event.	
Monitor Rule 7	uint32	The ID of the seventh monitor rule associated with the connection event.	
Monitor Rule 8	uint32	The ID of the eighth monitor rule associated with the connection event.	
Security Intelligence Source/ Destination	uint8	Whether the source or destination IP address matched the IP blacklist.	
Security Intelligence Layer	uint8	The IP layer that matched the IP blacklist.	

Connection Statistics Data Block 5.2.x

The connection statistics data block is used in connection data messages. Changes to the connection data block between versions 5.1.1 and 5.2 include the addition of new fields to support geolocation. The connection statistics data block for version 5.2.x has a block type of 144 in the series 1 group of blocks. It deprecates block type 137, Connection Statistics Data Block 5.1.1.x, page B-110.

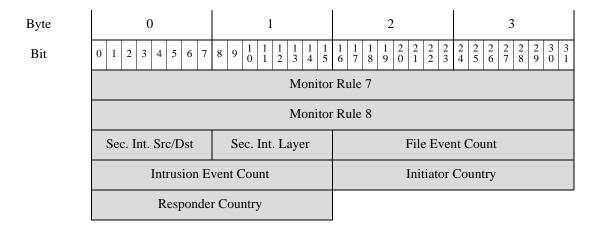
For more information on the Connection Statistics Data message, see Connection Statistics Data Message, page 4-45.

The following diagram shows the format of a Connection Statistics data block for 5.2.x:

Byte	0 1 2 3					
Bit	0 1 2 3 4 5 6 7 8 9 1 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1					
	Connection Data Block Type (144)					
	Connection Data Block Length					
	Device ID					
	Ingress Zone					
	Ingress Zone, continued					
	Ingress Zone, continued					
	Ingress Zone, continued					
	Egress Zone					
	Egress Zone, continued Egress Zone, continued Egress Zone, continued					
	Ingress Interface					
	Ingress Interface, continued					
	Ingress Interface, continued					
	Ingress Interface, continued					
	Egress Interface					
	Egress Interface, continued					
	Egress Interface, continued					
	Egress Interface, continued					
	Initiator IP Address					

Byte	0 1		2	3	
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1	
	Initiator IP Address, continued				
	Initiator IP Address, continued				
		Initiator IP Add	lress, continued		
		Responder	IP Address		
		Responder IP Ad	ldress, continued		
		Responder IP Ad	ldress, continued		
		Responder IP Ad	ldress, continued		
		Policy R	Revision		
		Policy Revision, continued			
	Policy Revision, continued				
	Policy Revision, continued				
	Rule ID				
	Rule Action Rule Reason				
	Initiator Port Responder Port				
	TCP Flags Protocol NetFlow Source			NetFlow Source	
	NetFlow Source, continued				
	NetFlow Source, continued				
	NetFlow Source, continued				
	NetFlow Source, continued Instance ID				
	Instance ID, cont. Connection Counter First Pkt Time				
	First Packet Timestamp, continued Last Pkt Time				
	Last Packet Timestamp, continued Initiator Tx Packets				
	Initiator Transmitted Packets, continued				
	Initiator Transmitted Packets, continued Resp. Tx Packets				
	Responder Transmitted Packets, continued				

Bit	Byte	0	1	2	3	
Initiator Transmitted Bytes, continued Initiator Transmitted Bytes, continued Responder Transmitted Bytes, continued Responder Transmitted Bytes, continued Responder Transmitted Bytes, continued User ID User ID, continued User ID Application Prot. ID Application Protocol ID, continued URL Category URL Category, continued URL Reputation URL Reputation, continued URL Reputation URL Reputation ID, continued Str. Block Type (0) String Block Type, continued String Block Type (0) String Block Length NetBIOS Name String Block Type (0) String Block Length NetBIOS Name Ctient App Version Ctient Application Version Monitor Rule 1 Monitor Rule 2 Monitor Rule 4 Monitor Rule 5	Bit	0 1 2 3 4 5 6 7	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1			
Initiator Transmitted Bytes, continued Responder Transmitted Bytes, continued Responder Transmitted Bytes, continued User ID User ID, continued User ID Application Protocol ID, continued URL Category URL Category, continued URL Reputation URL Reputation, continued URL Reputation URL Reputation ID, continued Str. Block Type (0) String Block Type, continued String Block Length String Block Length NetBIOS Name Client App Version String Block Type (0) String Block Type (0) String Block Length Client Application Version Client App Version Monitor Rule 1 Monitor Rule 3 Monitor Rule 5		Responder Transmitted Packets, continued Initiator Tx Bytes				
Responder Transmitted Bytes, continued Responder Transmitted Bytes, continued User ID User ID, continued User ID Application Prot. ID Application Protocol ID, continued URL Category URL Category, continued URL Reputation URL Reputation URL Reputation ID, continued Client App ID Client Application ID, continued Str. Block Type (0) String Block Type, continued String Block Length String Block Type (0) Monitor Rule 1 Monitor Rule 3 Monitor Rule 5		Initiator Transmitted Bytes, continued				
Responder Transmitted Bytes, continued User ID User ID, continued Application Prot. ID Application Protocol ID, continued URL Category URL Category, continued URL Reputation URL Reputation URL Reputation ID, continued Client App ID Client Application ID, continued Web App ID Str. Block Type (0) String Block Type, continued String Block Length String Block Length String Block Type (0) String Block Type (0) String Block Type (0) String Block Length NetBIOS Name Client App Version Client Application Version Monitor Rule 1 Monitor Rule 2 Monitor Rule 5		Initiato	r Transmitted Bytes, co	ontinued	Resp. Tx Bytes	
User ID, continued Application Prot. ID Application Protocol ID, continued URL Category URL Category, continued URL Reputation URL Reputation, continued Client App ID Client Application ID, continued Web App ID Client Web Application ID, continued Str. Block Type (0) String Block Type, continued String Block Length String Block Length, continued Client App. URL NetBIOS Name String Block Length NetBIOS Name Client App Version String Block Type (0) String Block Length NetBIOS Name Client App Version String Block Length Client Application Version Monitor Rule 1 Monitor Rule 2 Monitor Rule 3 Monitor Rule 4 Monitor Rule 5			Responder Transmit	ted Bytes, continued		
Application Protocol ID, continued URL Category URL Category, continued URL Reputation Str. Block Type (0) String Block Type, continued String Block Length NetBIOS Name Client App Version String Block Length NetBIOS Name Client App Version String Block Length Client Application Version Monitor Rule 1 Monitor Rule 2 Monitor Rule 3 Monitor Rule 5		Respond	ler Transmitted Bytes, o	continued	User ID	
URL Category, continued URL Reputation URL Reputation URL Reputation URL App ID Client Application ID, continued Web App ID Client URL String Block Type, continued String Block Type (0) String Block Length String Block Length Client App. URL NetBIOS Name String Block Length NetBIOS Name Client App Version Client App Version String Block Length Client Application Version Monitor Rule 1 Monitor Rule 3 Monitor Rule 4 Monitor Rule 5						
URL Reputation, continued Client App ID Client Application ID, continued Web App ID Client URL Web Application ID, continued Str. Block Type (0) String Block Type, continued Client App. URL NetBIOS Name String Block Length, continued Client App. URL NetBIOS Name Client App Version Client App Version Client Application Version Monitor Rule 1 Monitor Rule 3 Monitor Rule 4 Monitor Rule 5		Applie	cation Protocol ID, con	tinued	URL Category	
Client Application ID, continued Web App ID Client URL Web Application ID, continued Str. Block Type (0) String Block Type, continued Client App. URL NetBIOS Name String Block Length, continued Client App. URL NetBIOS Name Client App Version Client App Version String Block Length String Block Type (0) String Block Type (0) String Block Length Client App Version Monitor Rule 1 Monitor Rule 2 Monitor Rule 4 Monitor Rule 5		U	JRL Category, continue	ed	URL Reputation	
Client URL String Block Type, continued String Block Length String Block Length, continued Client App. URL NetBIOS Name String Block Length String Block Type (0) String Block Length NetBIOS Name Client App Version String Block Type (0) String Block Type (0) String Block Length NetBIOS Name Client App Version Monitor Rule 1 Monitor Rule 2 Monitor Rule 3 Monitor Rule 4 Monitor Rule 5		URL Reputation, continued Client App ID				
URL String Block Type, continued String Block Length String Block Length, continued Client App. URL NetBIOS Name String Block Type (0) String Block Length NetBIOS Name Client App Version String Block Type (0) String Block Type (0) String Block Type (0) String Block Type (1) Monitor Rule 1 Monitor Rule 2 Monitor Rule 3 Monitor Rule 4 Monitor Rule 5		Clier	Web App ID			
String Block Type, continued String Block Length String Block Length, continued Client App. URL NetBIOS Name String Block Type (0) String Block Length NetBIOS Name Client App Version String Block Type (0) String Block Type (0) String Block Length Client Application Version Monitor Rule 1 Monitor Rule 2 Monitor Rule 3 Monitor Rule 4 Monitor Rule 5		Web Application ID, continued			Str. Block Type (0)	
NetBIOS Name String Block Type (0) String Block Length NetBIOS Name Client App Version String Block Type (0) String Block Type (0) String Block Length Client Application Version Monitor Rule 1 Monitor Rule 2 Monitor Rule 3 Monitor Rule 4 Monitor Rule 5	OKE	String Block Type, continued				
Name String Block Length NetBIOS Name Client App Version String Block Type (0) String Block Length Client Application Version Monitor Rule 1 Monitor Rule 2 Monitor Rule 3 Monitor Rule 4 Monitor Rule 5		String Block Length, continued Client App			Client App. URL	
String Block Length NetBIOS Name Client App Version String Block Type (0) String Block Length Client Application Version Monitor Rule 1 Monitor Rule 2 Monitor Rule 3 Monitor Rule 4 Monitor Rule 5		String Block Type (0)				
Client App Version String Block Type (0) String Block Length Client Application Version Monitor Rule 1 Monitor Rule 2 Monitor Rule 3 Monitor Rule 4 Monitor Rule 5						
App Version String Block Length Client Application Version Monitor Rule 1 Monitor Rule 2 Monitor Rule 3 Monitor Rule 4 Monitor Rule 5		NetBIOS Name				
String Block Length Client Application Version Monitor Rule 1 Monitor Rule 2 Monitor Rule 3 Monitor Rule 4 Monitor Rule 5	Client App Version	String Block Type (0)				
Monitor Rule 1 Monitor Rule 2 Monitor Rule 3 Monitor Rule 4 Monitor Rule 5		String Block Length Client Application Version				
Monitor Rule 2 Monitor Rule 3 Monitor Rule 4 Monitor Rule 5						
Monitor Rule 3 Monitor Rule 4 Monitor Rule 5						
Monitor Rule 4 Monitor Rule 5		Monitor Rule 2				
Monitor Rule 5		Monitor Rule 4				
Monitor Rule 6						
		Monitor Rule 6				



The following table describes the fields of the Connection Statistics data block for 5.2.x:

Table B-23 Connection Statistics Data Block 5.2.x Fields

Field	Data Type	Description
Connection Statistics Data Block Type	uint32	Initiates a Connection Statistics data block for 5.2.x. The value is always 144.
Connection Statistics Data Block Length	uint32	Number of bytes in the Connection Statistics data block, including eight bytes for the connection statistics block type and length fields, plus the number of bytes in the connection data that follows.
Device ID	uint32	The device that detected the connection event.
Ingress Zone	uint8[16]	Ingress security zone in the event that triggered the policy violation.
Egress Zone	uint8[16]	Egress security zone in the event that triggered the policy violation.
Ingress Interface	uint8[16]	Interface for the inbound traffic.
Egress Interface	uint8[16]	Interface for the outbound traffic.
Initiator IP Address	uint8[16]	IP address of the host that initiated the session described in the connection event, in IP address octets.
Responder IP Address	uint8[16]	IP address of the host that responded to the initiating host, in IP address octets.
Policy Revision	uint8[16]	Revision number of the rule associated with the triggered correlation event, if applicable.
Rule ID	uint32	Internal identifier for the rule that triggered the event, if applicable.
Rule Action	uint16	The action selected in the user interface for that rule (allow, block, and so forth).
Rule Reason	uint16	The reason the rule triggered the event.
Initiator Port	uint16	Port used by the initiating host.
Responder Port	uint16	Port used by the responding host.
TCP Flags	uint16	Indicates any TCP flags for the connection event.

Table B-23 Connection Statistics Data Block 5.2.x Fields (continued)

Field	Data Type	Description	
Protocol	uint8	The IANA-specified protocol number.	
NetFlow Source	uint8[16]	IP address of the NetFlow-enabled device that exported the data for the connection.	
Instance ID	uint16	Numerical ID of the Snort instance on the managed device that generated the event.	
Connection Counter	uint16	Value used to distinguish between connection events that happen during the same second.	
First Packet Timestamp	uint32	UNIX timestamp of the date and time the first packet was exchanged in the session.	
Last Packet Timestamp	uint32	UNIX timestamp of the date and time the last packet was exchanged in the session.	
Initiator Transmitted Packets	uint64	Number of packets transmitted by the initiating host.	
Responder Transmitted Packets	uint64	Number of packets transmitted by the responding host.	
Initiator Transmitted Bytes	uint64	Number of bytes transmitted by the initiating host.	
Responder Transmitted Bytes	uint64	Number of bytes transmitted by the responding host.	
User ID	uint32	Internal identification number for the user who last logged into the host that generated the traffic.	
Application Protocol ID	uint32	Application ID of the application protocol.	
URL Category	uint32	The internal identification number of the URL category.	
URL Reputation	uint32	The internal identification number for the URL reputation.	
Client Application ID	uint32	The internal identification number of the detected client application, if applicable.	
Web Application ID	uint32	The internal identification number of the detected web application, if applicable.	
String Block Type	uint32	Initiates a String data block for the client application URL. This value is always 0.	
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 client application URL string.	
Client Application URL	string	URL the client application accessed, if applicable (/files/index.html, for example).	
String Block Type	uint32	Initiates a String data block for the host NetBIOS name. This value is always 0.	
String Block Length	uint32	Number of bytes in the String data block, including eight bytes for the string block type and length fields, plus the number of bytes in the NetBIOS name string.	

Table B-23 Connection Statistics Data Block 5.2.x Fields (continued)

Field	Data Type	Description	
NetBIOS Name	string	Host NetBIOS name string.	
String Block Type	uint32	Initiates a String data block for the client application version. This value is always 0.	
String Block Length	uint32	Number of bytes in the String data block for the client application version, including eight bytes for the string block type and length, plus the number of bytes in the version.	
Client Application Version	string	Client application version.	
Monitor Rule 1	uint32	The ID of the first monitor rule associated with the connection event.	
Monitor Rule 2	uint32	The ID of the second monitor rule associated with the connection event.	
Monitor Rule 3	uint32	The ID of the third monitor rule associated with the connection event.	
Monitor Rule 4	uint32	The ID of the fourth monitor rule associated with the connection event.	
Monitor Rule 5	uint32	The ID of the fifth monitor rule associated with the connection event.	
Monitor Rule 6	uint32	The ID of the sixth monitor rule associated with the connection event.	
Monitor Rule 7	uint32	The ID of the seventh monitor rule associated with the connection event.	
Monitor Rule 8	uint32	The ID of the eighth monitor rule associated with the connection event.	
Security Intelligence Source/ Destination	uint8	Whether the source or destination IP address matched the IP blacklist.	
Security Intelligence Layer	uint8	The IP layer that matched the IP blacklist.	
File Event Count	uint16	Value used to distinguish between file events that happen during the same second.	
Intrusion Event Count	uint16	Value used to distinguish between intrusion events that happen during the same second.	
Initiator Country	uint16	Code for the country of the initiating host.	
Responder Country	uint16	Code for the country of the responding host.	

Connection Chunk Data Block for 5.0 - 5.1

The Connection Chunk data block conveys connection data detected by a NetFlow device. The Connection Chunk data block has a block type of 66 for pre-4.10.1 versions. For versions 5.0 - 5.1, it has a block type of 119.

The following diagram shows the format of the Connection Chunk data block:

By te	0	1	2	3			
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1			
		Connection Chunk B	lock Type (66 119)				
	Connection Chunk Block Length						
	Initiator IP Address						
	Responder IP Address						
	Start Time						
	Application ID						
	Responder Port Protocol Connection Type						
	NetFlow Detector IP Address						
		Packets Sent					
	Packets Received						
	Bytes Sent						
		Bytes Received					
		Connections					

The following table describes the components of the Connection Chunk data block:

Table B-24 Connection Chunk Data Block Fields

Field	Data Type	Description	
Connection Chunk Block Type	uint32	Initiates a Connection Chunk data block. This value is 66 for versions before 4.10.1 and a value of 119 for version 5.0.	
Connection Chunk Block Length	uint32	Total number of bytes in the Connection Chunk data block, including eight bytes for the connection chunk block type and length fields, plus the number of bytes in the connection chunk data that follows.	
Initiator IP Address	uint8[4]	IP address of the host that initiated the connection, in IP address octets.	
Responder IP Address	uint8[4]	IP address of the host responding in the connection, in IP address octets.	
Start Time	uint32	The starting time for the connection chunk.	
Application ID	uint32	Application identification number for the application protocol used in the connection.	

Table B-24 Connection Chunk Data Block Fields (continued)

Field	Data Type	Description
Responder Port	uint16	The port used by the responder in the connection chunk.
Protocol	uint8	The protocol for the packet containing the user information.
Connection Type	uint8	The type of connection.
Source Device IP Address	uint8[4]	IP address of the NetFlow device that detected the connection, in IP address octets.
Packets Sent	uint32	The number of packets sent in the connection chunk.
Packets Received	uint32	The number of packets received in the connection chunk.
Bytes Sent	uint32	The number of bytes sent in the connection chunk.
Bytes Received	uint32	The number of bytes received in the connection chunk.
Connections	uint32	The number of sessions made in the connection chunk.

Connection Statistics Data Block 5.1.1.x

Byte

Bit

The connection statistics data block is used in connection data messages. Changes to the connection data block between versions 5.1 and 5.1.1 include the addition of new fields to identify associated intrusion events. The connection statistics data block for version 5.1.1.x has a block type of 137. It deprecates block type 126, Connection Statistics Data Block 5.1, page B-97.

For more information on the Connection Statistics Data message, see Connection Statistics Data Message, page 4-45.

The following diagram shows the format of a Connection Statistics data block for 5.1.1:

0	1	2	3				
0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 3 3 4 5 6 7 8 9 0 1				
	Connection Data Block Type (137)						
	Connection Dat	a Block Length					
	Devic	ee ID					
Ingress Zone							
Ingress Zone, continued							
Ingress Zone, continued							
Ingress Zone, continued							
Egress Zone							
Egress Zone, continued							
Egress Zone, continued							

FireSIGHT eStreamer Integration Guide

Byte	0	1	2	3				
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 1 8 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1				
	Egress Zone, continued							
		Ingress l	nterface					
		Ingress Interfa	ace, continued					
		Ingress Interfa	ace, continued					
		Ingress Interfa	ace, continued					
		Egress I	nterface					
	Egress Interface, continued							
	Egress Interface, continued							
	Egress Interface, continued							
	Initiator IP Address							
	Initiator IP Address, continued							
	Initiator IP Address, continued							
	Initiator IP Address, continued							
	Responder IP Address							
	Responder IP Address, continued							
		Responder IP Ad	ldress, continued					
		Responder IP Ac	ldress, continued					
		Policy F						
		Policy Revisi						
		Policy Revisi						
		Policy Revisi						
		Rule						
	Rule Action Rule Reason							
	Initiator Port Responder Port							
	TCP I		Protocol	NetFlow Source				
		NetFlow Sour	rce, continued	NetFlow Source, continued				

Instance ID, cont. Connection Counter First First Packet Timestamp, continued Last Last Packet Timestamp, continued Initiator Transmitted Packets, continued	t Pkt Time Pkt Time tiator Tx Packets
NetFlow Source, continued NetFlow Source, continued Instance ID, cont. Connection Counter First First Packet Timestamp, continued Last Last Packet Timestamp, continued Initiator Transmitted Packets, continued	t Pkt Time Pkt Time tiator Tx Packets
NetFlow Source, continued Instance ID, cont. Connection Counter First First Packet Timestamp, continued Last Last Packet Timestamp, continued Initiator Transmitted Packets, continued	t Pkt Time Pkt Time tiator Tx Packets
Instance ID, cont. Connection Counter First First Packet Timestamp, continued Last Last Packet Timestamp, continued Initiator Transmitted Packets, continued	t Pkt Time Pkt Time tiator Tx Packets
First Packet Timestamp, continued Last Packet Timestamp, continued Initiator Transmitted Packets, continued	Pkt Time tiator Tx Packets
Last Packet Timestamp, continued Initiator Transmitted Packets, continued	tiator Tx Packets
Initiator Transmitted Packets, continued	Packets
	Ty Doolests
Initiator Transmitted Dealecte continued	Ty Doolests
Resp.	Tx Packets
Responder Transmitted Packets, continued	
Responder Transmitted Packets, continued Initiate	or Tx Bytes
Initiator Transmitted Bytes, continued	
Initiator Transmitted Bytes, continued Resp	o. Tx Bytes
Responder Transmitted Bytes, continued	
Responder Transmitted Bytes, continued U	Jser ID
User ID, continued Applie	cation Prot. ID
Application Protocol ID, continued URL	L Category
URL Category, continued URL	Reputation
URL Reputation, continued Clien	nt App ID
Client Application ID, continued Wel	b App ID
Client Web Application ID, continued Str. Blo	ock Type (0)
String Block Type, continued Stri	ng Block Length
String Block Length, continued Client	App. URL
NetBIOS Name String Block Type (0)	
String Block Length	
NetBIOS Name	

Byte	0	1	2	3
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1
Client App Version		String Bloc	k Type (0)	
ripp version		String Blo	ck Length	
		Client Applica	tion Version	
	Monitor Rule 1			
	Monitor Rule 2			
	Monitor Rule 3			
	Monitor Rule 4			
	Monitor Rule 5			
	Monitor Rule 6			
	Monitor Rule 7			
	Monitor Rule 8			
	Sec. Int. Src/Dst Sec. Int. Layer File Event Count			ent Count
	Intrusion E	vent Count		

The following table describes the fields of the Connection Statistics data block for 5.1.1.x.

Table B-25 Connection Statistics Data Block 5.1.1.x Fields

Field	Data Type	Description	
Connection Statistics Data Block Type	uint32	Initiates a Connection Statistics data block for 5.1.1.x. The value is always 137.	
Connection Statistics Data Block Length	uint32	Number of bytes in the Connection Statistics data block, includin eight bytes for the connection statistics block type and length fields, plus the number of bytes in the connection data that follows.	
Device ID	uint32	The device that detected the connection event.	
Ingress Zone	uint8[16]	Ingress security zone in the event that triggered the policy violation.	
Egress Zone	uint8[16]	Egress security zone in the event that triggered the policy violation.	
Ingress Interface	uint8[16]	Interface for the inbound traffic.	
Egress Interface	uint8[16]	Interface for the outbound traffic.	

Table B-25 Connection Statistics Data Block 5.1.1.x Fields (continued)

Field	Data Type	Description	
Initiator IP Address	uint8[16]	IP address of the host that initiated the session described in the connection event, in IP address octets.	
Responder IP Address	uint8[16]	IP address of the host that responded to the initiating host, in IP address octets.	
Policy Revision	uint8[16]	Revision number of the rule associated with the triggered correlation event, if applicable.	
Rule ID	uint32	Internal identifier for the rule that triggered the event, if applicable.	
Rule Action	uint16	The action selected in the user interface for that rule (allow, block, and so forth).	
Rule Reason	uint16	The reason the rule triggered the event.	
Initiator Port	uint16	Port used by the initiating host.	
Responder Port	uint16	Port used by the responding host.	
TCP Flags	uint16	Indicates any TCP flags for the connection event.	
Protocol	uint8	The IANA-specified protocol number.	
NetFlow Source	uint8[16]	IP address of the NetFlow-enabled device that exported the data for the connection.	
Instance ID	uint16	Numerical ID of the Snort instance on the managed device that generated the event.	
Connection Counter	uint16	Value used to distinguish between connection events that happen during the same second.	
First Packet Timestamp	uint32	UNIX timestamp of the date and time the first packet was exchanged in the session.	
Last Packet Timestamp	uint32	UNIX timestamp of the date and time the last packet was exchanged in the session.	
Initiator Transmitted Packets	uint64	Number of packets transmitted by the initiating host.	
Responder Transmitted Packets	uint64	Number of packets transmitted by the responding host.	
Initiator Transmitted Bytes	uint64	Number of bytes transmitted by the initiating host.	
Responder Transmitted Bytes	uint64	Number of bytes transmitted by the responding host.	
User ID	uint32	Internal identification number for the user who last logged into the host that generated the traffic.	
Application Protocol ID	uint32	Application ID of the application protocol.	
URL Category	uint32	The internal identification number of the URL category.	
URL Reputation	uint32	The internal identification number for the URL reputation.	

Table B-25 Connection Statistics Data Block 5.1.1.x Fields (continued)

Field	Data Type	Description	
Client Application ID	uint32	The internal identification number of the detected client application, if applicable.	
Web Application ID	uint32	The internal identification number of the detected web application, if applicable.	
String Block Type	uint32	Initiates a String data block for the client application URL. This value is always 0.	
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 client application URL string.	
Client Application URL	string	URL the client application accessed, if applicable (/files/index.html, for example).	
String Block Type	uint32	Initiates a String data block for the host NetBIOS name. This value is always 0.	
String Block Length	uint32	Number of bytes in the String data block, including eight bytes for the string block type and length fields, plus the number of bytes in the NetBIOS name string.	
NetBIOS Name	string	Host NetBIOS name string.	
String Block Type	uint32	Initiates a String data block for the client application version. This value is always 0.	
String Block Length	uint32	Number of bytes in the String data block for the client application version, including eight bytes for the string block type and length, plus the number of bytes in the version.	
Client Application Version	string	Client application version.	
Monitor Rule 1	uint32	The ID of the first monitor rule associated with the connection event.	
Monitor Rule 2	uint32	The ID of the second monitor rule associated with the connection event.	
Monitor Rule 3	uint32	The ID of the third monitor rule associated with the connection event.	
Monitor Rule 4	uint32	The ID of the fourth monitor rule associated with the connection event.	
Monitor Rule 5	uint32	The ID of the fifth monitor rule associated with the connection event.	
Monitor Rule 6	uint32	The ID of the sixth monitor rule associated with the connection event.	
Monitor Rule 7	uint32	The ID of the seventh monitor rule associated with the connection event.	
Monitor Rule 8	uint32	The ID of the eighth monitor rule associated with the connection event.	

Table B-25 Connection Statistics Data Block 5.1.1.x Fields (continued)

Field	Data Type	Description
Security Intelligence Source/ Destination	uint8	Whether the source or destination IP address matched the IP blacklist.
Security Intelligence Layer	uint8	The IP layer that matched the IP blacklist.
File Event Count	uint16	Value used to distinguish between file events that happen during the same second.
Intrusion Event Count	uint16	Value used to distinguish between intrusion events that happen during the same second.

Connection Statistics Data Block 5.3

The connection statistics data block is used in connection data messages. Changes to the connection data block between versions 5.2.x and 5.3 include the addition of new fields for NetFlow information. The connection statistics data block for version 5.3 has a block type of 152 in the series 1 group of blocks. It deprecates block type 144, Connection Statistics Data Block 5.2.x, page B-103.

You request connection event records by setting the extended event flag—bit 30 in the Request Flags field—in the request message with an event version of 10 and an event code of 71. See Request Flags, page 2-11. If you enable bit 23, an extended event header is included in the record.

For more information on the Connection Statistics Data message, see Connection Statistics Data Message, page 4-45.

The following diagram shows the format of a Connection Statistics data block for 5.3+:

Byte	0	1	2	3	
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1	
	Connection Data Block Type (152)				
	Connection Data Block Length				
	Device ID				
	Ingress Zone				
	Ingress Zone, continued				
	Ingress Zone, continued				
	Ingress Zone, continued				
	Egress Zone				
	Egress Zone, continued				

Byte	0	1	2	3						
Bit	0 1 2 3 4 5 6 7 8 9 1 1 1 2 3 4 5 6 7 8 9 0 1 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0									
		Egress Zone	e, continued							
		Egress Zone	e, continued							
		Ingress I	nterface							
		Ingress Interfa	ice, continued							
		Ingress Interfa	ice, continued							
		Ingress Interfa	ice, continued							
		Egress I	nterface							
		Egress Interfa	ce, continued							
		Egress Interfa	ce, continued							
		Egress Interfa	ce, continued							
		Initiator II								
		Initiator IP Add								
		Initiator IP Add								
		Initiator IP Add								
		Responder								
		Responder IP Ad								
		Responder IP Ad								
		Responder IP Ad								
		Policy R								
		Policy Revision								
		Policy Revision								
	Policy Revision, continued									
	Rule /	Rule ID Rule Action Rule Reason								
	Initiato		Respond							
			Protocol	NetFlow Source						
	TCP Flags Protocol NetFlow Source									

Byte	0	3						
Bit	0 1 2 3 4 5 6 7	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1						
		NetFlow Source	ce, continued					
		NetFlow Source	ce, continued					
		NetFlow Source	ce, continued					
	No	etFlow Source, continue	ed	Instance ID				
	Instance ID, cont.	Connection	n Counter	First Pkt Time				
	First I	Packet Timestamp, conti	inued	Last Pkt Time				
	Last I	Packet Timestamp, conti	nued	Initiator Tx Packets				
		Initiator Transmitted	Packets, continued					
	Initiator	Transmitted Packets, co	ontinued	Resp. Tx Packets				
		Responder Transmitted	d Packets, continued					
	Responde	r Transmitted Packets, c	continued	Initiator Tx Bytes				
		Initiator Transmitted	d Bytes, continued					
	Initiato	r Transmitted Bytes, cor	ntinued	Resp. Tx Bytes				
		Responder Transmitte	ed Bytes, continued					
	Respond	er Transmitted Bytes, co	ontinued	User ID				
		User ID, continued		Application Prot. ID				
	Applio	cation Protocol ID, conti	inued	URL Category				
	U	TRL Category, continued	l	URL Reputation				
	Ul	RL Reputation, continue	ed	Client App ID				
	Clier	nt Application ID, contin	nued	Web App ID				
Client URL	Web	Application ID, continu	ued	Str. Block Type (0)				
	Str	ing Block Type, continu	ed	String Block Length				
	Strii	ng Block Length, contin	ued	Client App. URL				

Byte	0	1	1 2 3							
Bit	0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2									
NetBIOS		String Block Type (0)								
Name		String Blo	ck Length							
		NetBIOS	Name							
Client App Version		String Bloo	ck Type (0)							
App version		String Blo	ck Length							
		Client Applica	tion Version							
		Monitor	r Rule 1							
		Monitor	r Rule 2							
		Monitor	r Rule 3							
		Monitor	r Rule 4							
		Monitor	r Rule 5							
		Monitor	r Rule 6							
		Monitor	r Rule 7							
		Monitor	r Rule 8							
	Sec. Int. Src/Dst	Sec. Int. Layer	File Ever	nt Count						
	Intrusion E	Intrusion Event Count Initiator Country								
	Responder Country IOC Number									
		Source Autonomous System								
		Destination Auto	onomous System							
	SNM	IP In	SNMI	P Out						
	Source TOS	Destination TOS	Source Mask	Destination Mask						

The following table describes the fields of the Connection Statistics data block for 5.3.

Table B-26 Connection Statistics Data Block 5.3+ Fields

Field	Data Type	Description
Connection Statistics Data Block Type	uint32	Initiates a Connection Statistics data block for 5.3. The value is always 152.
Connection Statistics Data Block Length	uint32	Number of bytes in the Connection Statistics data block, including eight bytes for the connection statistics block type and length fields, plus the number of bytes in the connection data that follows.
Device ID	uint32	The device that detected the connection event.
Ingress Zone	uint8[16]	Ingress security zone in the event that triggered the policy violation.
Egress Zone	uint8[16]	Egress security zone in the event that triggered the policy violation.
Ingress Interface	uint8[16]	Interface for the inbound traffic.
Egress Interface	uint8[16]	Interface for the outbound traffic.
Initiator IP Address	uint8[16]	IP address of the host that initiated the session described in the connection event, in IP address octets.
Responder IP Address	uint8[16]	IP address of the host that responded to the initiating host, in IP address octets.
Policy Revision	uint8[16]	Revision number of the rule associated with the triggered correlation event, if applicable.
Rule ID	uint32	Internal identifier for the rule that triggered the event, if applicable.
Rule Action	uint16	The action selected in the user interface for that rule (allow, block, and so forth).
Rule Reason	uint16	The reason the rule triggered the event.
Initiator Port	uint16	Port used by the initiating host.
Responder Port	uint16	Port used by the responding host.
TCP Flags	uint16	Indicates any TCP flags for the connection event.
Protocol	uint8	The IANA-specified protocol number.
NetFlow Source	uint8[16]	IP address of the NetFlow-enabled device that exported the data for the connection.
Instance ID	uint16	Numerical ID of the Snort instance on the managed device that generated the event.
Connection Counter	uint16	Value used to distinguish between connection events that happen during the same second.
First Packet Timestamp	uint32	UNIX timestamp of the date and time the first packet was exchanged in the session.
Last Packet Timestamp	uint32	UNIX timestamp of the date and time the last packet was exchanged in the session.

Table B-26 Connection Statistics Data Block 5.3+ Fields (continued)

Field	Data Type	Description
Initiator Transmitted Packets	uint64	Number of packets transmitted by the initiating host.
Responder Transmitted Packets	uint64	Number of packets transmitted by the responding host.
Initiator Transmitted Bytes	uint64	Number of bytes transmitted by the initiating host.
Responder Transmitted Bytes	uint64	Number of bytes transmitted by the responding host.
User ID	uint32	Internal identification number for the user who last logged into the host that generated the traffic.
Application Protocol ID	uint32	Application ID of the application protocol.
URL Category	uint32	The internal identification number of the URL category.
URL Reputation	uint32	The internal identification number for the URL reputation.
Client Application ID	uint32	The internal identification number of the detected client application, if applicable.
Web Application ID	uint32	The internal identification number of the detected web application, if applicable.
String Block Type	uint32	Initiates a String data block for the client application URL. This value is always 0.
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 client application URL string.
Client Application URL	string	URL the client application accessed, if applicable (/files/index.html, for example).
String Block Type	uint32	Initiates a String data block for the host NetBIOS name. This value is always 0.
String Block Length	uint32	Number of bytes in the String data block, including eight bytes for the string block type and length fields, plus the number of bytes in the NetBIOS name string.
NetBIOS Name	string	Host NetBIOS name string.
String Block Type	uint32	Initiates a String data block for the client application version. This value is always 0.
String Block Length	uint32	Number of bytes in the String data block for the client application version, including eight bytes for the string block type and length, plus the number of bytes in the version.
Client Application Version	string	Client application version.

Table B-26 Connection Statistics Data Block 5.3+ Fields (continued)

Field	Data Type	Description
Monitor Rule 1	uint32	The ID of the first monitor rule associated with the connection event.
Monitor Rule 2	uint32	The ID of the second monitor rule associated with the connection event.
Monitor Rule 3	uint32	The ID of the third monitor rule associated with the connection event.
Monitor Rule 4	uint32	The ID of the fourth monitor rule associated with the connection event.
Monitor Rule 5	uint32	The ID of the fifth monitor rule associated with the connection event.
Monitor Rule 6	uint32	The ID of the sixth monitor rule associated with the connection event.
Monitor Rule 7	uint32	The ID of the seventh monitor rule associated with the connection event.
Monitor Rule 8	uint32	The ID of the eighth monitor rule associated with the connection event.
Security Intelligence Source/ Destination	uint8	Whether the source or destination IP address matched the IP blacklist.
Security Intelligence Layer	uint8	The IP layer that matched the IP blacklist.
File Event Count	uint16	Value used to distinguish between file events that happen during the same second.
Intrusion Event Count	uint16	Value used to distinguish between intrusion events that happen during the same second.
Initiator Country	uint16	Code for the country of the initiating host.
Responder Country	uint 16	Code for the country of the responding host.
IOC Number	uint16	ID Number of the compromise associated with this event.
Source Autonomous System	uint32	Autonomous system number of the source, either origin or peer.
Destination Autonomous System	uint32	Autonomous system number of the destination, either origin or peer.
SNMP Input	uint16	SNMP index of the input interface.
SNMP Output	uint16	SNMP index of the output interface.
Source TOS	uint8	Type of Service byte setting for the incoming interface.
Destination TOS	uint8	Type of Service byte setting for the outgoing interface.

Table B-26 Connection Statistics Data Block 5.3+ Fields (continued)

Field	Data Type	Description
Source Mask	uint8	Source address prefix mask.
Destination Mask	uint8	Destination address prefix mask.

Connection Statistics Data Block 5.3.1

The connection statistics data block is used in connection data messages. The only changes to the connection data block between versions 5.3 and 5.3.1 is the addition of a security context field. The connection statistics data block for version 5.3.1 has a block type of 154 in the series 1 group of blocks. It deprecates block type 152, Connection Statistics Data Block 5.3, page B-116.

You request connection event records by setting the extended event flag—bit 30 in the Request Flags field—in the request message with an event version of 11 and an event code of 71. See Request Flags, page 2-11. If you enable bit 23, an extended event header is included in the record. For more information on the Connection Statistics Data message, see Connection Statistics Data Message, page 4-45.

The following diagram shows the format of a Connection Statistics data block for 5.3.1:

Byte	0	0 1 2 3									
Bit	0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2										
		Connection Data I	Block Type (154)								
		Connection Data	a Block Length								
		Devic	re ID								
		Ingress	Zone								
		Ingress Zone	e, continued								
		Ingress Zone	e, continued								
		Ingress Zone	e, continued								
		Egress	Zone								
		Egress Zone	, continued								
		Egress Zone	, continued								
	Egress Zone, continued										
	Ingress Interface										
	Ingress Interface, continued										
	Ingress Interface, continued										
		Ingress Interfa	ce, continued								

Byte	0		2 3												
Bit	0 1 2 3 4 5 6 7	8 9 1	1 1 1 2	1 3	1 1 4 5	1 6	1 1 7 8	$\begin{bmatrix} 1 & 2 \\ 9 & 0 \end{bmatrix}$	2 1	2 2	2 2	2 2 5	2 2 6 7	2 2 8	2 3 3 0 1
	Egress Interface														
			Egre	ss Ir	iterfa	ice,	conti	nued							
			Egre	ss Ir	iterfa	ice,	conti	nued							
			Egre	ss Ir	terfa	ice,	conti	nued							
			I	nitia	tor I	P A	ddres	S							
		Iı	nitiat	or IP	Add	lres	s, coi	itinue	d						
							s, coi								
		Iı					s, coi		d						
				_			Addro								
			•				ess, co								
			_				ess, co								
		Re	spon				ess, co	ontinu	ied						
			D. 1'				ision	1							
							conti								
							conti								
			1 0110	- X	Rule			iiucu							
	Rule A	Action							F	Rule	Re	ason			
	Initiato	or Port										er Poi	t		
	TCP I	Flags					P	rotoc	ol			Net	Flov	v Sou	ırce
			NetF	Flow	Sou	rce,	conti	nued							
		NetFlow Source, continued NetFlow Source, continued													
	NetFlow Source, continued														
	NetFlow Source, continued Instance ID														
	Instance ID, cont.		(Conn	ectio	n C	Count	er				Fii	st P	kt Tir	ne
	First P	acket Ti	mest	amp,	, con	tinu	ied					La	st Pl	kt Tir	ne

Byte		0					1						2				3					
Bit	0 1 2	0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 3									2 2 4	2 2 6	2 2	2 2	2 2 9	3 0	3					
			Las	st P	acket	Tim	estan	np, c	ont	inu	ed						Initiator Tx Packets					
					Init	tiatoı	Trai	ısmi	ted	Pa	cke	ets, c	onti	nue	d	_						
]	Initiat	or [Frans	mitte	ed Pa	ckets	s, co	onti	nu	ed					Resp	. T	x F	Pack	ets	
					Resp	ond	er Tra	ansm	itte	d P	acl	xets,	con	tinu	ed							
		R	espon	der	Tran	smit	ted P	acke	ts,	con	tin	ued					Initia	tor	Ty	к Ву	tes	
							or Tra						ontin	ued								
			Initia	tor													Res	р. Т	Гх	Byt	es	
						•	ler T				Ĭ		conti	nue	d							
		I	Respo	nde						onti	inu	ed						Use				
					Use	r ID,	cont	inue	d 								Application Prot. ID					
			App	olic	ation	Prot	ocol	ID, o	ont	inu	ed						URL Category					
				U	RL C	atego	ory, c	onti	nue	d							URL Reputation					
				UR	L Re	puta	tion,	cont	inu	ed							Client App ID					
			Cl	ien	t App	licat	ion I	D, co	nti	nue	d						Web App ID					
Client URL			W	/eb	Appl	icati	on II), co	ntin	uec	1						Str. Block Type (0))	
			S	Strii	ng Bl	ock '	Гуре,	con	tinu	ied							Stı	ing Le	g B ng	lock th	ζ	
			St	rin	g Blo	ck L	engtl	ı, co	ntin	uec	d					(Client	: A _j	pp.	. UR	L	
NetBIOS Name							Stri	ng B	loc	k T	уре	e (0)										
							Str	ing l	Bloo	ck I	Len	gth										
							N	etBI	OS	Na	me	·										
Client App Version								ng B														
	String Block Length																					
		Client Application Version																				
								Mon														
								Mon	itor	Ku	ile '	2										

Byte

Bit

2 0 1 3 2 3 Monitor Rule 3 Monitor Rule 4 Monitor Rule 5 Monitor Rule 6 Monitor Rule 7 Monitor Rule 8 Sec. Int. Src/Dst Sec. Int. Layer File Event Count **Intrusion Event Count Initiator Country** Responder Country **IOC** Number Source Autonomous System **Destination Autonomous System** SNMP In **SNMP Out** Source TOS **Destination TOS** Source Mask **Destination Mask** Security Context Security Context, continued Security Context, continued Security Context, continued

The following table describes the fields of the Connection Statistics data block for 5.3.1.

Table B-27 Connection Statistics Data Block 5.3.1 Fields

Field	Data Type	Description
Connection Statistics Data Block Type	uint32	Initiates a Connection Statistics data block for 5.3.1+. The value is always 154.
Connection Statistics Data Block Length	uint32	Number of bytes in the Connection Statistics data block, including eight bytes for the connection statistics block type and length fields, plus the number of bytes in the connection data that follows.
Device ID	uint32	The device that detected the connection event.

Table B-27 Connection Statistics Data Block 5.3.1 Fields (continued)

Field	Data Type	Description
Ingress Zone	uint8[16]	Ingress security zone in the event that triggered the policy violation.
Egress Zone	uint8[16]	Egress security zone in the event that triggered the policy violation.
Ingress Interface	uint8[16]	Interface for the inbound traffic.
Egress Interface	uint8[16]	Interface for the outbound traffic.
Initiator IP Address	uint8[16]	IP address of the host that initiated the session described in the connection event, in IP address octets.
Responder IP Address	uint8[16]	IP address of the host that responded to the initiating host, in IP address octets.
Policy Revision	uint8[16]	Revision number of the rule associated with the triggered correlation event, if applicable.
Rule ID	uint32	Internal identifier for the rule that triggered the event, if applicable.
Rule Action	uint16	The action selected in the user interface for that rule (allow, block, and so forth).
Rule Reason	uint16	The reason the rule triggered the event.
Initiator Port	uint16	Port used by the initiating host.
Responder Port	uint16	Port used by the responding host.
TCP Flags	uint16	Indicates any TCP flags for the connection event.
Protocol	uint8	The IANA-specified protocol number.
NetFlow Source	uint8[16]	IP address of the NetFlow-enabled device that exported the data for the connection.
Instance ID	uint16	Numerical ID of the Snort instance on the managed device that generated the event.
Connection Counter	uint16	Value used to distinguish between connection events that happen during the same second.
First Packet Timestamp	uint32	UNIX timestamp of the date and time the first packet was exchanged in the session.
Last Packet Timestamp	uint32	UNIX timestamp of the date and time the last packet was exchanged in the session.
Initiator Transmitted Packets	uint64	Number of packets transmitted by the initiating host.
Responder Transmitted Packets	uint64	Number of packets transmitted by the responding host.
Initiator Transmitted Bytes	uint64	Number of bytes transmitted by the initiating host.
Responder Transmitted Bytes	uint64	Number of bytes transmitted by the responding host.

Table B-27 Connection Statistics Data Block 5.3.1 Fields (continued)

Field	Data Type	Description
User ID	uint32	Internal identification number for the user who last logged into the host that generated the traffic.
Application Protocol ID	uint32	Application ID of the application protocol.
URL Category	uint32	The internal identification number of the URL category.
URL Reputation	uint32	The internal identification number for the URL reputation.
Client Application ID	uint32	The internal identification number of the detected client application, if applicable.
Web Application ID	uint32	The internal identification number of the detected web application, if applicable.
String Block Type	uint32	Initiates a String data block for the client application URL. This value is always 0.
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 client application URL string.
Client Application URL	string	URL the client application accessed, if applicable (/files/index.html, for example).
String Block Type	uint32	Initiates a String data block for the host NetBIOS name. This value is always 0.
String Block Length	uint32	Number of bytes in the String data block, including eight bytes for the string block type and length fields, plus the number of bytes in the NetBIOS name string.
NetBIOS Name	string	Host NetBIOS name string.
String Block Type	uint32	Initiates a String data block for the client application version. This value is always 0.
String Block Length	uint32	Number of bytes in the String data block for the client application version, including eight bytes for the string block type and length, plus the number of bytes in the version.
Client Application Version	string	Client application version.
Monitor Rule 1	uint32	The ID of the first monitor rule associated with the connection event.
Monitor Rule 2	uint32	The ID of the second monitor rule associated with the connection event.
Monitor Rule 3	uint32	The ID of the third monitor rule associated with the connection event.
Monitor Rule 4	uint32	The ID of the fourth monitor rule associated with the connection event.
Monitor Rule 5	uint32	The ID of the fifth monitor rule associated with the connection event.

Table B-27 Connection Statistics Data Block 5.3.1 Fields (continued)

Field	Data Type	Description
Monitor Rule 6	uint32	The ID of the sixth monitor rule associated with the connection event.
Monitor Rule 7	uint32	The ID of the seventh monitor rule associated with the connection event.
Monitor Rule 8	uint32	The ID of the eighth monitor rule associated with the connection event.
Security Intelligence Source/ Destination	uint8	Whether the source or destination IP address matched the IP blacklist.
Security Intelligence Layer	uint8	The IP layer that matched the IP blacklist.
File Event Count	uint16	Value used to distinguish between file events that happen during the same second.
Intrusion Event Count	uint16	Value used to distinguish between intrusion events that happen during the same second.
Initiator Country	uint16	Code for the country of the initiating host.
Responder Country	uint 16	Code for the country of the responding host.
IOC Number	uint16	ID Number of the compromise associated with this event.
Source Autonomous System	uint32	Autonomous system number of the source, either origin or peer.
Destination Autonomous System	uint32	Autonomous system number of the destination, either origin or peer.
SNMP Input	uint16	SNMP index of the input interface.
SNMP Output	uint16	SNMP index of the output interface.
Source TOS	uint8	Type of Service byte setting for the incoming interface.
Destination TOS	uint8	Type of Service byte setting for the outgoing interface.
Source Mask	uint8	Source address prefix mask.
Destination Mask	uint8	Destination address prefix mask.
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.

Legacy File Event Data Structures

The following topics describe other legacy file event data structures:

• File Event for 5.1.1.x, page B-130

- File Event for 5.2.x, page B-134
- File Event for 5.3, page B-138
- File Event for 5.3.1, page B-144
- File Event SHA Hash for 5.1.1-5.2.x, page B-150

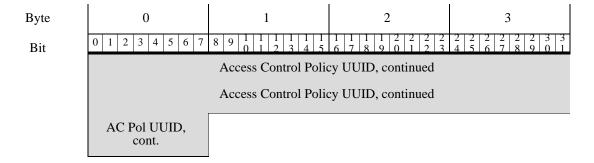
File Event for 5.1.1.x

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 23 in the series 2 group of blocks.

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 1 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1										
		File Event Blo	ock Type (23)											
		File Event B	lock Length											
		Devic	ee ID											
	Connection Instance Connection Counter													
	Connection Timestamp													
	File Event Timestamp													
		Source IP Address												
		Source IP Addr	ress, continued											
		Source IP Addr	ress, continued											
		Source IP Addr	ress, continued											
		Destination	IP Address											
		Destination IP Ad	ldress, continued											
		Destination IP Ac	ldress, continued											
		Destination IP Ac	ldress, continued											
	Disposition	Action	SHA	Hash										

Byte	0	1	2	3										
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1										
		SHA Hash,	continued											
		SHA Hash,	continued											
	0 1 2 3 4 5 6 7 8 9 1 1 2 3 14 5 6 7 8 9 1 1 2 3 14 5 6 7 8 9 0 1 1 2 3 14 5 6 7 8 9 0 1 1 2 3 14 5 6 7 8 9 0 1 1 2 3 3 4 5 6 7 8 9 0 1 1 2 3 3 4 5 6 7 8 9 0 1 1 2 3 3 4 5 6 7 8 9 0 1 1 2 3 3 4 5 6 7 8 9 0 1 1 2 3 3 4 5 6 7 8 9 0 1 1 2 3 3 4 5 6 7 8 9 0 0 1 1 2 2 3 3 4 5 6 7 8 8 9 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1													
	SHA Hash, continued SHA Hash, continued SHA Hash, continued SHA Hash, continued SHA Hash, continued SHA Hash, continued SHA Hash, continued File Type ID File Type ID, cont. String Block Type (0) String Block Type (0), cont. String Block Length String Block Length, cont. File Size File Size File Size, continued Direction Application ID App ID, cont. User ID User ID, cont. String Block Type (0) String Block Type (0) String Block Length													
	SHA Hash	, continued	File Ty	ype ID										
File Name	File Type	ID, cont.	String Bloc	ek Type (0)										
	String Block 7	Гуре (0), cont.	String Blo	ck Length										
	String Block	Length, cont.	File Name											
	File Size													
		File Size,	continued											
	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 Bloc	k Type (0)											
	SHA Hash, continued SHA Hash, continued SHA Hash, continued SHA Hash, continued SHA Hash, continued SHA Hash, continued File Type ID File Type ID String Block Type (0) String Block Type (0), cont. File Name File Size File Size, continued Direction Application ID App ID, cont. User ID User ID, cont. String Block Type (0) String Block Type (0) String Block Length CIRI String Block Type (0) String Block Length Signature													
		Signat	ture											
	Source	SHA Hash, continued SHA Ha												
	SHA Hash, continued SHA Hash, continued SHA Hash, continued SHA Hash, continued SHA Hash, continued SHA Hash, continued String Block Type (0) String Block Type (0), cont. String Block Length Size File Size File Size, continued Direction Application ID App ID, cont. User ID User ID, cont. String Block Type (0) String Block Type (0) String Block Length String Block Length String Block Length String Block Length Signature Source Port Destination Port													
		Access Control Police	cy UUID, continued											



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

Table B-28 File Event Data Block Fields

Field	Data Type	Description
File Event Block Type	uint32	Initiates whether file event data block. This value is always 23.
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 — CACHE_MISS — The software was unable to send a request to the Cisco cloud for a disposition.
		• 5 — NO_CLOUD_RESP — The Cisco cloud services did not respond to the request.

Table B-28 File Event Data Block Fields (continued)

Field	Data Type	Description						
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						
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.						
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	following values: • 1 — Detect • 2 — Block • 3 — Malware Cloud Lookup • 4 — Malware Block • 5 — Malware Whitelist SHA-256 hash of the file, in binary format. ID number that maps to the file type. Name of the file. Size of the file in bytes. 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).						
URI	string	Uniform Resource Identifier (URI) of the connection.						
Signature	string	SHA-256 hash of the file, in binary format. ID number that maps to the file type. Name of the file. Size of the file in bytes. 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). ID number that maps to the application using the file transfer. ID number for the user logged into the destination host, as identified by the system. Uniform Resource Identifier (URI) of the connection. SHA-256 hash of the file, in string format. Port number for the source of the connection. Port number for the destination of the connection. IANA protocol number specified by the user. For example:						
Source Port	uint16	following values: • 1 — Detect • 2 — Block • 3 — Malware Cloud Lookup • 4 — Malware Block • 5 — Malware Whitelist SHA-256 hash of the file, in binary format. ID number that maps to the file type. Name of the file. Size of the file in bytes. 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). ID number that maps to the application using the file transfer. ID number for the user logged into the destination host, as identified by the system. Uniform Resource Identifier (URI) of the connection. SHA-256 hash of the file, in string format. Port number for the source of the connection. Port number for the destination of the connection. IANA protocol number specified by the user. For example: • 1 — ICMP • 4 — IP • 6 — TCP • 17 — UDP This is currently only TCP. Unique identifier for the access control policy that triggered the						
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]							

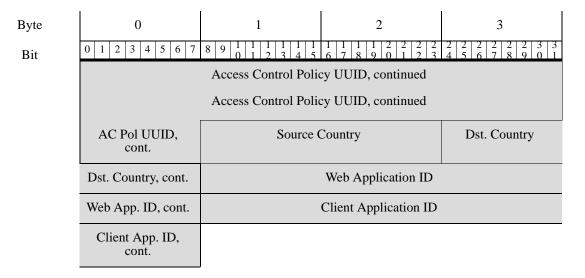
File Event for 5.2.x

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 32 in the series 2 group of blocks. It supersedes block type 23. New fields have been added to track source and destination country, as well as the client and web application instances.

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 1 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1											
		File Event Blo	ock Type (32)												
		File Event B	lock Length												
		Devic	ee ID												
	Connection	Connection Instance Connection Counter													
	Connection Timestamp														
	File Event Timestamp														
	Source IP Address														
		Source IP Addr	ress, continued												
		Source IP Addr	ress, continued												
		Source IP Addr	ress, continued												
		Destination	IP Address												
		Destination IP Ad	ldress, continued												
		Destination IP Ac	ldress, continued												
		Destination IP Ac	ldress, continued												
	Disposition	Action	SHA	Hash											

Byte	0	1	2	3										
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1										
		SHA Hash,	continued											
		SHA Hash,	continued											
	SHA Hash, continued SHA Ha													
	SHA Hash, continued SHA Hash, continued SHA Hash, continued File Type ID File Type ID, cont. String Block Type (0) String Block Type (0), cont. String Block Length String Block Length, cont. File Size File Size, continued Direction Application ID													
	SHA Hash	, continued	File Ty	pe ID										
File Name	File Type	ID, cont.	String Bloc	ek Type (0)										
	String Block 7	Гуре (0), cont.	String Block Length											
	String Block	Length, cont.	File Name											
	File Size													
		File Size,	continued											
	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 Bloc	k Type (0)											
		String Blo	ck Length											
		Signat	ture											
	O I 2 3 4 5 6 7 8 9 1 1 1 2 3 4 1 5 6 7 8 9 1 1 2 3 4 1 5 6 7 8 9 0 1 1 2 3 4 5 6 7 8 9 0 1 1 2 3 4 5 6 7 8 9 0 1 1 2 3 4 5 6 7 7 8 9 0 1 1 2 1 2 3 4 4 1 2 1 2 1 2 2 2 2 1 2 2 2 2 2 2 2 2													
	SHA Hash, continued SHA Hash, continued SHA Hash, continued File Type ID 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 User ID String Block Type (0) String Block Type (0) String Block Length String Block Length String Block Length Signature Source Port Destination Port													
		Access Control Police	cy UUID, continued											



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

Table B-29 File Event Data Block Fields

Field	Data Type	Description
File Event Block Type	uint32	Initiates whether file event data block. This value is always 23.
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.

Table B-29 File Event Data Block 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 — NEUTRAL — It is unknown whether the file contains malware.			
		• 3 — MALWARE — The file contains malware.			
		 4 — CACHE_MISS — 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. 			
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			
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.			
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	1 — CLEAN — The file is clean and does not contain malware. 2 — NEUTRAL — It is unknown whether the file contain malware. 3 — MALWARE — The file contains malware. 4 — CACHE_MISS — The software was unable to send request to the Cisco cloud for a disposition, or the Cisco cloud services did not respond to the request. The action taken on the file based on the file type. Can have following values: 1 — Detect 2 — Block 3 — Malware Cloud Lookup 4 — Malware Block 5 — Malware Whitelist SHA-256 hash of the file, in binary format. ID number that maps to the file type. Name of the file. Size of the file in bytes. 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 connection is HTTP it is a download). ID number that maps to the application using the file transfer of the user logged into the destination host, as identified by the system. Juliform Resource Identifier (URI) of the connection. SHA-256 hash of the file, in string format. Port number for the source of the connection.			
User ID	uint32				
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.			

Table B-29 File Event Data Block Fields (continued)

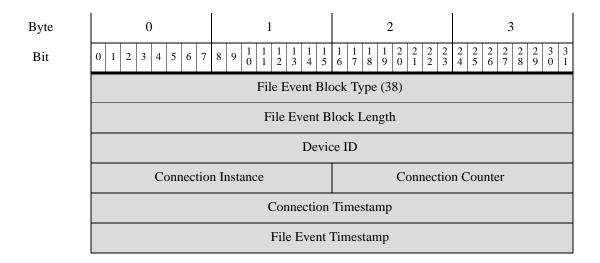
Field	Data Type	Description
Protocol	uint8	IANA protocol number specified by the user. For example:
		• 1 — ICMP
		• 4 — IP
		• 6 — TCP
		• 17 — UDP
		This is currently only TCP.
Access Control Policy UUID	uint8[16]	Unique identifier for the access control policy that triggered the event.
Source Country	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.

File Event for 5.3

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 38 in the series 2 group of blocks. It supersedes block type 32. New fields have been added to track dynamic file analysis and file storage.

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 3 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					ĺ	2								3									
Bit	0 1	2	3 4	8	8 9)	1 0	1 1	1 2	13	1 4	1 5	1 6	1 5 7		1 1 2)	2 2	2 2		2 2 4	2	2 5	2 6	2 7	2 8	2 :	3 :	3 1			
												S	ou	ırce	e II	P <i>A</i>	Add	re	ess													
										So	uı	rce	IF	P A	dc	lre	ss,	cc	nti	nu	ed											
																			nti													
										So	uı	rce	IF	P A	.dc	lre	SS,	cc	nti	nu	ed											
		Destination IP Address																														
	Destination IP Address, continued																															
	Destination IP Address, continued																															
	Destination IP Address, continued																															
		Dis	posi	tio	on				D	SP Disp				Į			File	e \$	Stor	ag	ge S	tatı	ıs			Fil		An	alys us	sis		
	Arc	hive	e Fil	e S	Statı	ıs		ı	Τŀ	hrea	at i	Sco	ore	е					A	cti	on					S	Н	A I	Hasl	h		
											,	SH	A	На	ısh	ı, c	ont	in	uec	l												
											,	SH	A	На	ısh	ı, c	ont	in	uec	l												
											,	SH	A	На	ısh	ı, c	ont	in	uec	l												
											,	SH	A	На	sh	ı, c	ont	in	uec	l												
											,	SH	A	На	sh	ı, c	ont	in	uec	l												
											,	SH	A	На	sh	ı, c	ont	in	uec	l												
												SH	Α	На	sh	ı, c	ont	in	uec	l												
							S	НА	ŀ	Has	h,	co	nti	inu	ed	l									File Type ID							
File Name								File	e T	Тур	e I	ID,	, c	ont	t.										String Block Type (0)							
						Stı	rir	ng E	3lo	ock	T	уре	e (0),	co	ont	•									St		ıg I eng	3loo gth	ck		
						St	ri	ng l	Bl	lock	ιI	Len	ıgt	h,	со	nt.										Fi	le	Na	me			
														F	ile	Si	ize															
												Fi	le	Siz	ze,	cc	nti	nı	ied													
		Di	recti	ior	1												A	p	plic	at	ion	ID										
	A	\pp	ID,	со	nt.														Us	er	ID											

Byte	0	1	2	3
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1
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			ion 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.			

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

Table B-30 File Event Data Block Fields

Field	Data Type	Description
File Event Block Type	uint32	Initiates whether file event data block. This value is always 23.
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.

Table B-30 File Event Data Block Fields (continued)

Field	Data Type	Description	
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.	
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 B-30 File Event Data Block Fields (continued)

Field	Data Type	Description	
File Analysis Status	uint8	Indicates whether the file was sent for dynamic analysis. Possible values are:	
		• 0 — File Not Sent for Analysis	
		• 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	
SHA Hash	uint8[32]	SHA-256 hash of the file, in binary format.	

Table B-30 File Event Data Block Fields (continued)

Field	Data Type	Description	
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 3-37 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.	

Byte

Bit

File Event for 5.3.1

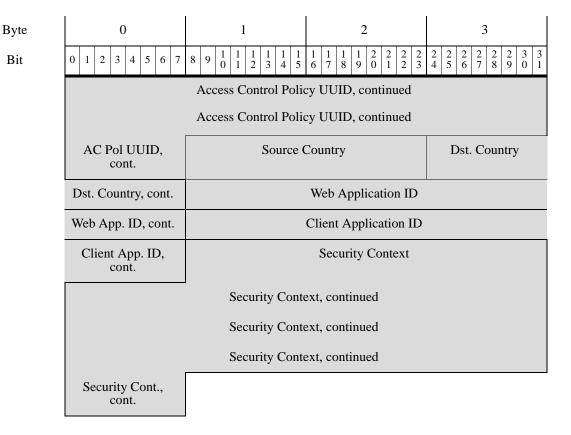
The file event contains information on files that are sent over the network. This includes the connection information, whether the file is malware, and specific information to identify the file. The file event has a block type of 43 in the series 2 group of blocks. It supersedes block type 38. A security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

0 1		2	3		
0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 1 5	1 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1		
	File Event Blo	ock Type (43)			
	File Event B	lock Length			
	Devi	ce ID			
Connection	n Instance	Connection Counter			
	Connection	Timestamp			
	File Event	Гimestamp			
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		

Byte	0	1	2	3						
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1						
		SHA Hash	, continued							
		SHA Hash	, continued							
		SHA Hash	, continued							
		SHA Hash	, continued							
			, continued							
			, continued							
		SHA Hash	, continued							
		SHA Hash, continued		File Type ID						
File Name		File Type ID, cont.		String Block Type (0)						
	Str	ring Block Type (0), co	ont.	String Block Length						
	St	ring Block Length, con	nt.	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 Bloo	ck Type (0)							
		String Blo	ock Length							
		Signa	iture							
	Source	e Port	Destina	tion Port						
	Protocol	Ac	cess Control Policy UU	JID						
		Access Control Poli	cy UUID, continued							



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

Table B-31 File Event Data Block 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.

Table B-31 File Event Data Block 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.
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 B-31 File Event Data Block Fields (continued)

Field	Data Type	Description
File Analysis Status	uint8	Indicates whether the file was sent for dynamic analysis. Possible values are:
		• 0 — File Not Sent for Analysis
		• 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
SHA Hash	uint8[32]	SHA-256 hash of the file, in binary format.

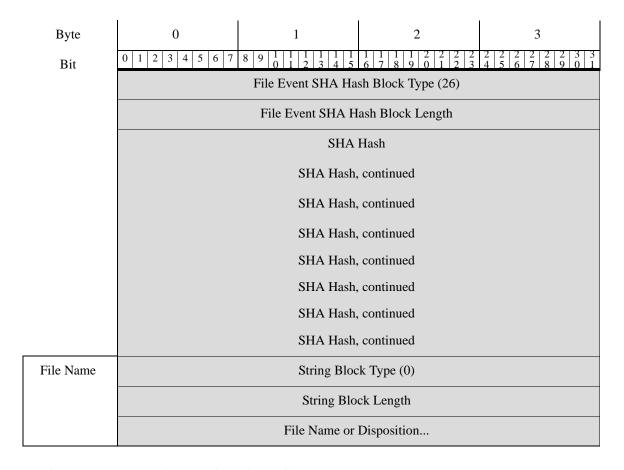
Table B-31 File Event Data Block Fields (continued)

Field	Data Type	Description
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 3-37 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.

File Event SHA Hash for 5.1.1-5.2.x

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 26 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 4 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 B-32 File Event SHA Hash 5.1.1-5.2.x 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.

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.
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.

Table B-32 File Event SHA Hash 5.1.1-5.2.x Data Block Fields (continued)

Legacy Correlation Event Data Structures

The following topics describe other legacy correlation (compliance) data structures:

- Correlation Event for 5.0 5.0.2, page B-151
- Correlation Event for 5.1-5.3.x, page B-159

Correlation Event for 5.0 - 5.0.2

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 116. Data block type 116 differs from its predecessor (block type 107) in including additional information about the associated security zone and interface.

You can request 5.0 correlation events from eStreamer only by extended request, for which you request event type code 31 and version code 7 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.

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 4-54.

By te				0)				1							2						3										
Bit	0	1	2	3	4	5	6	7	8	9	1	1	1 2	1 3	1 4	1 5	1 6	1 7	1 8	1 9	2	2	2	2 3	2 4	2 5	2 6	2 7	2 8	2	3	3
					Н	lea	deı	Ve	ersi	on	(1))									N	Лes	ssa	ge	Ту	pe	(4)	1				
	Message Length																															
													R	lec	ord	Ту	pe	(1	12))												
														Re	eco	rd :	Lei	ngt	h													
		eStreamer Server Timestamp (in events, only if bit 23 is set)																														
							Re	ser	veo	d fo	or F	₹ut	ure	U	se (in	eve	ent	s, c	onl	y if	`bi	t 2	3 is	s se	et)						

By te	0	1	2	3	
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 1 8 9 0 1 2 3 4 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1	
		Correlation Blo			
		Correlation I	Block Length		
		Devid	ce ID		
		(Correlation)	Event Second		
		Ever	nt ID		
		Polic	ey ID		
		Rule	e ID		
		Prio	prity		
		String Bloo	ck Type (0)		Event Description
		String Blo	ock Length		Description
		Description		Event Type	
		Event De	evice ID		
		Signat	ure ID		
		Signature G	enerator ID		
		(Trigger) Ev	vent Second		
		(Trigger) Even	nt Microsecond		
		Ever	nt ID		
		Event Def	ined Mask		
	Event Impact Flags	IP Protocol	Network	Protocol	
		Sour	ce IP		
	Source Host Type	Source V	LAN ID	Source OS Fprt UUID	Source OS Fprt UUID
		Source OS Fingerpri	int UUID, continued		
		Source OS Fingerpri	int UUID, continued		
		Source OS Fingerpri	int UUID, continued		
	Source O	S Fingerprint UUID, c	continued	Source Criticality	

By te

Bit

	()			1								2	2			3							ĺ
0 1	2 3	4	5 6	7	8	9 $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$		1 1 2 3	1 4	1 5		1 1 7 8	1 9	2	2	$\begin{bmatrix} 2 & 2 \\ 2 & 3 \end{bmatrix}$	2 4	2 5	2 6	2 7	2 8	2 9		3
Sou		riti ont	cality	′,							S	Sour	ce I	Use	r I	D								
So		Use	er ID,					Š	Sou	rce	Po	rt					,	Sou	ırc	e S	erv	er]	ID	
				Sou	ırce	Serv	er I	D, co	onti	nu	ed							D	est	ina	tio	n II)	
				D	esti	natio	n IF	, cor	ntin	uec	i							De	st.	Н	st '	Тур	e	
			Dest.	VI	LAN	1 ID						De	stin	atio	on	OS F	ing	gerj	pri	nt I	JU	ID		
]	Dest	tinati	on (OS F	ing	erp	rint	: UU	ID,	, co	nti	nued								
]	Dest	tinati	on (OS F	ing	erp	rint	UU	ID,	, co	nti	nued								
]	Dest	tinati	on (OS F	ing	erp	rint	UU	ID,	, co	nti	nued								
I	Destii	nati	on OS		nge		nt U	UID,	,]	Des	stir	ation	C:	riti	cal	ity				
								D	est.	U	ser	ID												
			Desti	nat	ion	Port								Des	stir	nation	S	erv	er	ID				
	De	stiı	nation	ı Se	rve	r ID,	con	ıt.			Blocked							Ingress Interface UUID						
						Ing	ress	Inte	rfac	e I	JUI	D, c	ont	inu	ed									
						Ing	ress	Inte	rfac	e U	JUI	D, c	ont	inu	ed									
					Ingress Interface U						UUID, continued													
			Ing	res	s Int	terfa	ce U	JUID), co	onti	inue	ed						Eg		ss I: UU	nte	rfac	ce	
						Egı	ess	Inter	rfac	e L	JUI	D, c	onti	inu	ed									
						Egr	ess	Inter	rfac	e L	JUI	D, c	onti	inu	ed									
Egress Interface							e L	JUI	D, c	onti	inu	ed												
Egress Interface UUID, con							nti	itinued							Ingress Zone UUID									
Ingress Z							Zo	Zone UUID																
Ingress Zone UUID,								D, continued																
							gre	ss Zo	one	UU	JID	, cor	ntin	uec	l									

Dest OS Fingerprint UUID

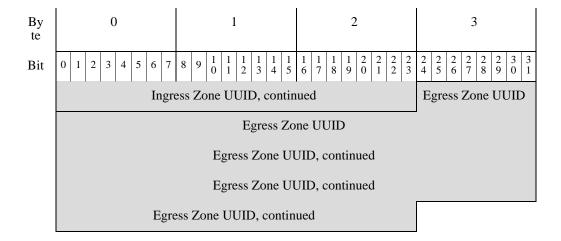


Table B-33 Correlation Event 5.0 - 5.0.2 Data Fields

Field	Data Type	Description
Correlation Block Type	uint32	Indicates a correlation event data block follows. This field always has a value of 107. See Understanding Discovery (Series 1) Blocks, page 4-54.
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 zero indicates the Defense Center. You can obtain managed device names by requesting Version 3 metadata. See Managed Device Record Metadata, page 3-32 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.
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 4-62.
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.

Table B-33 Correlation Event 5.0 - 5.0.2 Data Fields (continued)

Field	Data Type	Description
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 3-32 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 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 B-34 on page B-158 for a list of each bit value.

Table B-33 Correlation Event 5.0 - 5.0.2 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 (bit 6). 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.
		The following impact level values map to specific priorities on the Defense Center. An x indicates the value can be 0 or 1:
		• (0, unknown): 00x00000
		• red (1, vulnerable): xxxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx
		• orange (2, potentially vulnerable): 00x00111
		• yellow (3, currently not vulnerable): 00x00011
		• 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	uint8[4]	IP address of the source host in the event, in IP address octets.
Source Host	uint8	Source host's type:
Type		• 0 — Host
		• 1 — Router
		• 2 — Bridge
Source VLAN ID	uint16	Source host's VLAN identification number, if applicable.

Table B-33 Correlation Event 5.0 - 5.0.2 Data Fields (continued)

Field	Data Type	Description
Source OS Fingerprint	uint8[16]	A fingerprint ID number that acts a unique identifier for the source host's operating system.
UUID		See Server Record, page 4-14 for information about obtaining the values that map to the fingerprint IDs.
Source	uint16	User-defined criticality value for the source host:
Criticality		• 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]	IP address of the destination host associated with the policy violation (if applicable). This value will be 0 if there is no destination IP address.
Destination	uint8	Destination host's type:
Host Type		• 0 — Host
		• 1 — Router
		• 2 — Bridge
Destination VLAN ID	uint16	Destination host's VLAN identification number, if applicable.
Destination OS Fingerprint	uint8[16]	A fingerprint ID number that acts as a unique identifier for the destination host's operating system.
UUID		See Server Record, page 4-14 for information about obtaining the values that map to the fingerprint IDs.
Destination	uint16	User-defined criticality value for the destination host:
Criticality		• 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 B-33 Correlation Event 5.0 - 5.0.2 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.

The following table describes each Event Defined Mask value.

Table B-34 Event Defined Values

Description	Mask Value
Event Impact Flags	0x0000001
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
Destination Criticality	0x00004000
Destination Port	0x00008000
Destination Server	0x00010000

Table B-34 Event Defined Values (continued)

Description	Mask Value
Source User	0x00020000
Destination User	0x00040000

Correlation Event for 5.1-5.3.x

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.

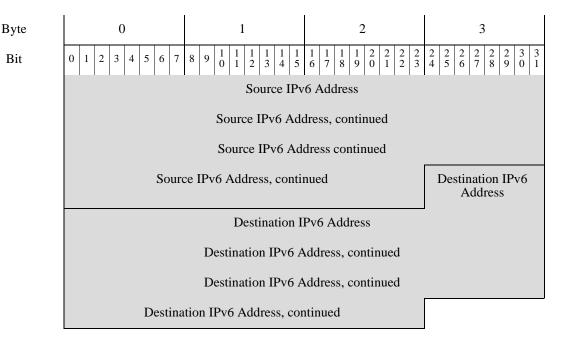
You can request 5.1-5.3.x correlation events from eStreamer only by extended request, for which you request event type code 31 and version code 8 in the Stream Request message (see Submitting Extended Requests, page 2-4 for information about submitting extended requests). You can optionally enable bit 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 1 1 1 1 1 1 1 5	1 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1	
	Header Ve	ersion (1)	Message	Type (4)	
		Message	Length		
		Record Ty	rpe (112)		
		Record I	Length		
	eStream	ner Server Timestamp (i	in events, only if bit 23	3 is set)	
	Reserved for Future Use (in events, only if bit 23 is set)				
	Correlation Block Type (128)				
	Correlation Block Length				
	Device ID				
	(Correlation) Event Second				
	Event ID				
	Policy ID				
	Rule ID				
		Prior	rity		

Byte	0	1	2	3	
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1	
		String Bloc	k Type (0)		Event Description
		String Bloo	ck Length		Bescription
		Description		Event Type	
		Event De	evice ID		
		Signati	ire ID		
		Signature G	enerator ID		
		(Trigger) Ev	rent Second		
		(Trigger) Even	t Microsecond		
		Even	t ID		
	Event Defined Mask				
	Event Impact Flags	IP Protocol	Network	Protocol	
		Sourc	ce IP		
	Source Host Type	Source V	LAN ID	Source OS Fprt UUID	Source OS Fprt UUID
		Source OS Fingerpri	nt UUID, continued		
		Source OS Fingerpri	nt UUID, continued		
	Source OS Fingerprint UUID, continued				
	Source OS Fingerprint UUID, continued Source Criticality				
	Source Criticality, cont Source User ID				
	Source User ID, cont	Source	e Port	Source Server ID	
	cont	Source arce Server ID, continu		Source Server ID Destination IP	

Byte	0 1	2	3	
Bit	0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1	
	Dest. VLAN ID	Destination OS F	ingerprint UUID	Dest OS Fingerprint
	Destination OS Finger	print UUID, continued		UUID
	Destination OS Finger	print UUID, continued		
	Destination OS Fingery	print UUID, continued		
	Destination OS Fingerprint UUID, continued	Destination	Criticality	
	Dest. U	Jser 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, cont	inued	Egress Interface UUID	
	Egress Interface UUID, continued			
	Egress Interface UUID, continued			
	Egress Interface U	UUID, continued		
	Egress Interface UUID, cont	inued	Ingress Zone UUID	
	Ingress Zo	one UUID		
	Ingress Zone U	UID, continued		
	Ingress Zone U	UID, continued		
	Ingress Zone UUID, contin	nued	Egress Zone UUID	
	Egress Zo	ne UUID		
	Egress Zone UU	UID, continued		
	Egress Zone UU	UID, continued		
	Egress Zone UUID, contin	ued	Source IPv6 Address	

Bit



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 4-54.

Table B-35 Correlation Event 5.1-5.3.x 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 4-54.
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 zero indicates the Defense Center. You can obtain managed device names by requesting Version 3 metadata. See Managed Device Record Metadata, page 3-32 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.
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.

Table B-35 Correlation Event 5.1-5.3.x Data Fields (continued)

Field	Data Type	Description	
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 4-62.	
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 3-32 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 B-34 on page B-158 for a list of each bit value.	

Table B-35 Correlation Event 5.1-5.3.x 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:
		• (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	uint8	Source host's type:
Type		• 0 — Host
		• 1 — Router
		• 2 — Bridge

Table B-35 Correlation Event 5.1-5.3.x Data Fields (continued)

Field	Data Type	Description
Source VLAN ID	uint16	Source host's VLAN identification number, if applicable.
Source OS Fingerprint	uint8[16]	A fingerprint ID number that acts a unique identifier for the source host's operating system.
UUID		See Server Record, page 4-14 for information about obtaining the values that map to the fingerprint IDs.
Source	uint16	User-defined criticality value for the source host:
Criticality		• 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	uint8	Destination host's type:
Host Type		• 0 — Host
		• 1 — Router
		• 2 — Bridge
Destination VLAN ID	uint16	Destination host's VLAN identification number, if applicable.
Destination OS Fingerprint	uint8[16]	A fingerprint ID number that acts as a unique identifier for the destination host's operating system.
UUID		See Server Record, page 4-14 for information about obtaining the values that map to the fingerprint IDs.
Destination	uint16	User-defined criticality value for the destination host:
Criticality		• 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 B-35 Correlation Event 5.1-5.3.x 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.	

Legacy Host Data Structures

To request these structures, you must use a Host Request Message. To request a legacy structure, the Host Request Message must use an older format. See Host Request Message Format, page 2-24 for more information.

The following topics describe legacy host data structures, including both host profile and full host profile structures:

- Full Host Profile Data Block 5.0 5.0.2, page B-166
- Full Host Profile Data Block 5.1.1, page B-176
- Full Host Profile Data Block 5.2.x, page B-184
- Host Profile Data Block for 5.1.x, page B-196
- IP Range Specification Data Block for 5.0 5.1.1.x, page B-202

Full Host Profile Data Block 5.0 - 5.0.2

The Full Host Profile data block for version 5.0 - 5.0.2 contains a full set of data describing one host. It has the format shown in the graphic below and explained in the following table. Note that, except for List data blocks, the graphic does not show the fields of the encapsulated data blocks. These encapsulated data blocks are described separately in Understanding Discovery & Connection Data Structures, page 4-1. The Full Host Profile data block a block type value of 111.



An asterisk(*) next to a block name in the following diagram indicates that multiple instances of the data block may occur.

Byte	0	0 1		3		
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 1 5	$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1		
		Full Host Profile	Data Block (111)			
		Data Blo	ck Length			
	IP Address					
	Hops Generic List Block Type (31)					
	Generic List Block Type, continued	G	eneric List Block Leng	gth		
OS Derived Fingerprints	Generic List Block Length, continued	Operating Sy	stem Fingerprint Block	k Type (130)*		
	OS Fingerprint Block Type (130)*, con't	Operating	System Fingerprint Blo	ock Length		
	OS Fingerprint Block Length, con't	Operating System Derived Fingerprint Data				
	Generic List Block Type (31)					
	Generic List Block Length					
Server Fingerprints	Ol	perating System Finge	rprint Block Type (130))*		
1 mgorprints	Operating System Fingerprint Block Length					
		Operating System Ser	ver Fingerprint Data			
		Generic List B	lock Type (31)			
		Generic List	Block Length			
Client Fingerprints	Operating System Fingerprint Block Type (130)*					
	Operating System Fingerprint Block Length					
		Operating System Cli	ent Fingerprint Data			
		Generic List B	lock Type (31)			
		Generic List	Block Length			

Byte	0	1	2	3				
Bit	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 3 3 3 3 3						
VDB Native Fingerprints 1	Operating System Fingerprint Block Type (130)*							
1 mgcrprimts 1	Operating System Fingerprint Block Length							
		Operating System VI	OB Fingerprint Data					
		Generic List Block Type (31)						
		Generic List	Block Length					
VDB Native Fingerprints 2	Ol	perating System Finger	rprint Block Type (130))*				
ringerprints 2		Operating System Fin	gerprint Block Length	ı				
		Operating System VI	OB Fingerprint Data					
		Generic List B	lock Type (31)					
		Generic List	Block Length					
User	Ol	perating System Finger	rprint Block Type (130))*				
ringerprints	Operating System Fingerprint Block Length Operating System User Fingerprint Data							
	Generic List Block Type (31)							
	Generic List Block Length							
Scan Fingerprints	Operating System Fingerprint Block Type (130)*							
Tingerprints		Operating System Fin	gerprint Block Length	ı				
		Operating System Sc	an Fingerprint Data					
		Generic List B	lock Type (31)					
		Generic List	Block Length					
Application Fingerprints	O _l	perating System Finger	rprint Block Type (130))*				
1 ingerprints		Operating System Fin	gerprint Block Length					
	Ol	perating System Applic	cation Fingerprint Dat	a				
		Generic List B	lock Type (31)					
		Generic List	Block Length					

Byte	0	1	2 3	
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 1 5	1 1 1 1 2 <td>3 3 0 1</td>	3 3 0 1
Conflict Fingerprints	Operating System Fingerprint Block Type (130)*			
1 mgcrprmts		Operating System Fir	gerprint Block Length	
	Operating System Conflict Fingerprint Data			
(TCP) Full Server Data		List Block	Type (11)	
Server Bata		List Block	k Length	
		(TCP) Full Server	Data Blocks (104)*	
(UDP) Full Server Data		List Block	Type (11)	
Server Data		List Bloo	ck Length	
		(UDP) Full Server	Data Blocks (104)*	
Network Protocol Data		List Block	Type (11)	
Trotocor Butta		List Bloo	ck Length	
		(Network) Protoco	ol Data Blocks (4)*	
Transport Protocol Data		List Block	Type (11)	
Trotocor Butu	List Block Length			
	(Transport) Protocol Data Blocks (4)*			
MAC Address Data		List Block	Type (11)	
Tradress Butu		List Bloo	ck Length	
		Host MAC Addres	s Data Blocks (95)*	
		Last	Seen	
		Host	Туре	
	Business Criticality VLAN ID			
	VLAN Type	VLAN Priority	Generic List Block Type (31)	
Host Client Data	Generic List Bloc	k Type, continued	Generic List Block Length	
Data	Generic List Block	Length, continued	Full Host Client Application Data Bloc (112)*	ks

Byte	0	1	2	3			
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 2 3 3 3 4 5 6 7 8 9 0 1			
NetBIOS Name		String Bloc	ek Type (0)				
1 (1111)		String Bloo	ck Length				
		NetBIOS Na	ame String				
Notes Data		String Bloc	ck Type (0)				
		String Bloo	ck Length				
		Notes St	tring				
(VDB) Host Vulns	Generic List Block Type (31)						
	Generic List Block Length						
	(VDB) Host Vulnerability Data Blocks (85)*						
3rd Pty/VDB) Host Vulns							
	Generic List Block Length						
	(Third Party/VDB) Host Vulnerability Data Blocks (85)*						
3rd Pty Scan Host Vulns		Generic List Bl	lock Type (31)				
	Generic List Block Length						
	(Third Party Scan) Host Vulnerability Data Blocks with Original Vuln IDs (85)*						
Attribute Value Data	List Block Type (11)						
		List Blocl	k Length				
		Attribute Value	Data Blocks *				

The following table describes the components of the Full Host Profile for 5.0 - 5.0.2 record.

Table B-36 Full Host Profile Record 5.0 - 5.0.2 Fields

Field	Data Type	Description	
IP Address	uint8[4]	IP address of the host, in IP address octets.	
Hops	uint8	Number of network hops from the host to the device.	
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data derived from the existing fingerprints for the host. This value is always 31.	

Table B-36 Full Host Profile Record 5.0 - 5.0.2 Fields (continued)

Field	Data Type	Description	
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.	
Operating System Derived Fingerprint Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host derived from the existing fingerprints for the host. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.	
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data identified using a server fingerprint. This value is always 31.	
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.	
Operating System Fingerprint (Server Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host identified using a server fingerprint. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.	
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data identified using a client fingerprint. This value is always 31.	
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.	
Operating System Fingerprint (Client Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host identified using a client fingerprint. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.	
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data identified using a Cisco VDB fingerprint. This value is always 31.	
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.	
Operating System Fingerprint (VDB) Native Fingerprint 1) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host identified using the fingerprints in the Cisco vulnerability database (VDB). See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.	

Table B-36 Full Host Profile Record 5.0 - 5.0.2 Fields (continued)

Field	Data Type	Description	
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data identified using a Cisco VDB fingerprint. This value is always 31.	
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.	
Operating System Fingerprint (VDB) Native Fingerprint 2) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host identified using the fingerprints in the Cisco vulnerability database (VDB). See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.	
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data added by a user. This value is always 31.	
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.	
Operating System Fingerprint (User Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host added by a user. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.	
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data added by a vulnerability scanner. This value is always 31.	
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.	
Operating System Fingerprint (Scan Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host added by a vulnerability scanner. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.	
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data added by an application. This value is always 31.	
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.	

Table B-36 Full Host Profile Record 5.0 - 5.0.2 Fields (continued)

Field	Data Type	Description
Operating System Fingerprint (Application Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host added by an application. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data selected through fingerprint conflict resolution. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.
Operating System Fingerprint (Conflict Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host selected through fingerprint conflict resolution. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.
List Block Type	uint32	Initiates a List data block comprising Full Server data blocks conveying TCP service data. This value is always 11.
List Block Length	uint32	Number of bytes in the list. This number includes the eight bytes of the list block type and length fields, plus the length of all encapsulated Full Server data blocks.
(TCP) Full Server Data Blocks *	variable	List of Full Server data blocks conveying data about the TCP services on the host. See Full Host Server Data Block 4.10.0+, page 4-125 for a description of this data block.
List Block Type	uint32	Initiates a List data block comprising Full Server data blocks conveying UDP service data. This value is always 11.
List Block Length	uint32	Number of bytes in the list. This number includes the eight bytes of the list block type and length fields, plus the length of all encapsulated Full Server data blocks.
(UDP) Full Server Data Blocks *	variable	List of Full Server data blocks conveying data about the UDP sub-servers on the host. See Full Host Server Data Block 4.10.0+, page 4-125 for a description of this data block.
List Block Type	uint32	Initiates a List data block comprising Protocol data blocks conveying network protocol data. This value is always 11.
List Block Length	uint32	Number of bytes in the list. This number includes the eight bytes of the list block type and length fields, plus the length of all encapsulated Protocol data blocks.
(Network) Protocol Data Blocks *	variable	List of Protocol data blocks conveying data about the network protocols on the host. See Protocol Data Block, page 4-67 for a description of this data block.
List Block Type	uint32	Initiates a List data block comprising Protocol data blocks conveying transport protocol data. This value is always 11.

Table B-36 Full Host Profile Record 5.0 - 5.0.2 Fields (continued)

Field	Data Type	Description	
List Block Length	uint32	Number of bytes in the list. This number includes the eight bytes of the list block type and length fields, plus the length of all encapsulated Protocol data blocks.	
(Transport) Protocol Data Blocks *	variable	List of Protocol data blocks conveying data about the transport protocols on the host. See Protocol Data Block, page 4-67 for a description of this data block.	
List Block Type	uint32	Initiates a List data block containing Host MAC Address data blocks. This value is always 11.	
List Block Length	uint32	Number of bytes in the list, including the list header and all encapsulated Host MAC Address data blocks.	
Host MAC Address Data Blocks *	variable	List of Host MAC Address data blocks. See Host MAC Address 4.9+, page 4-105 for a description of this data block.	
Last Seen	uint32	UNIX timestamp that represents the last time the system detected host activity.	
Host Type	uint32	Indicates host type. Values include:	
		• 0 — Host	
		• 1 — Router	
		• 2 — Bridge	
		• 3 — NAT (network address translation device)	
		• 4 — LB (load balancer)	
Business Criticality	uint16	Indicates criticality of host to business.	
VLAN ID	uint16	VLAN identification number that indicates which VLAN the host is a member of.	
VLAN Type	uint8	Type of packet encapsulated in the VLAN tag.	
VLAN Priority	uint8	Priority value included in the VLAN tag.	
Generic List Block Type	uint32	Initiates a Generic List data block comprising Host Vulnerability data blocks conveying Client Application data. This value is always 31.	
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Client Application data blocks.	
Full Host Client Application Data Blocks *	variable	List of Client Application data blocks. See Full Host Client Application Data Block 5.0+, page 4-139 for a description of this data block.	
String Block Type	uint32	Initiates a String data block for the host NetBIOS name. This value is always 0.	
String Block Length	uint32	Number of bytes in the String data block, including eight bytes for the string block type and length fields, plus the number of bytes in the NetBIOS name string.	
NetBIOS Name	string	Host NetBIOS name string.	

Table B-36 Full Host Profile Record 5.0 - 5.0.2 Fields (continued)

Field	Data Type	Description	
String Block Type	uint32	Initiates a String data block for host notes. This value is always 0.	
String Block Length	uint32	Number of bytes in the notes String data block, including eight bytes for the string block type and length fields, plus the number of bytes in the notes string.	
Notes	string	Contains the contents of the Notes host attribute for the host.	
Generic List Block Type	uint32	Initiates a Generic List data block comprising Host Vulnerability data blocks conveying VDB vulnerability data. This value is always 31.	
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated data blocks.	
(VDB) Host Vulnerability Data Blocks *	variable	List of Host Vulnerability data blocks for vulnerabilities identified in the Cisco vulnerability database (VDB). See Host Vulnerability Data Block 4.9.0+, page 4-103 for a description of this data block.	
Generic List Block Type	uint32	Initiates a Generic List data block comprising Host Vulnerability data blocks conveying third-party scan vulnerability data. This value is always 31.	
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated data blocks.	
(Third Party/VDB) Host Vulnerability Data Blocks *	variable	Host Vulnerability data blocks sourced from a third party scanner and containing information about host vulnerabilities cataloged in the Cisco vulnerability database (VDB). See Host Vulnerability Data Block 4.9.0+, page 4-103 for a description of this data block.	
Generic List Block Type	uint32	Initiates a Generic List data block comprising Host Vulnerability data blocks conveying third party scan vulnerability data. This value is always 31.	
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated data blocks.	
(Third Party Scan) Host Vulnerability Data Blocks *	variable	Host Vulnerability data blocks sourced from a third party scanner. Note that the host vulnerability IDs for these data blocks are the third party scanner IDs, not Cisco-detected IDs. See Host Vulnerability Data Block 4.9.0+, page 4-103 for a description of this data block.	
List Block Type	uint32	Initiates a List data block comprising Attribute Value data blocks conveying attribute data. This value is always 11.	
List Block Length	uint32	Number of bytes in the List data block, including the list header and all encapsulated data blocks.	
Attribute Value Data Blocks *	variable	List of Attribute Value data blocks. See Attribute Value Data Block, page 4-73 for a description of the data blocks in this list.	

Full Host Profile Data Block 5.1.1

The Full Host Profile data block for version 5.1.1 contains a full set of data describing one host. It has the format shown in the graphic below and explained in the following table. Note that, except for List data blocks, the graphic does not show the fields of the encapsulated data blocks. These encapsulated data blocks are described separately in Understanding Discovery & Connection Data Structures, page 4-1. The Full Host Profile data block a block type value of 135. It deprecates data block 111.



An asterisk(*) next to a block name in the following diagram indicates that multiple instances of the data block may occur.

Byte	0	0 1		3		
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1		
	Full Host Profile Data Block (135)					
	Data Block Length					
		IP Address				
	Hops	Ge	neric List Block Type	(31)		
	Generic List Block Type, continued	G	eneric List Block Leng	gth		
OS Derived Fingerprints	Generic List Block Length, continued	k Type (130)*				
	OS Fingerprint Block Type (130)*, con't Operating System Fingerprint Block Le		ock Length			
	OS Fingerprint Block Length, con't	Operating S	System Derived Finger	print Data		
		Generic List B	lock Type (31)			
		Generic List	Block Length			
Server Fingerprints	Operating System Fingerprint Block Type (130)*					
1 mgc prims	Operating System Fingerprint Block Length					
		Operating System Ser	ver Fingerprint Data			
		Generic List B	lock Type (31)			
		Generic List	Block Length			

Byte	0	1	2	3	
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1	
Client Fingerprints	Operating System Fingerprint Block Type (130)*				
ringcipinits	Operating System Fingerprint Block Length				
	Operating System Client Fingerprint Data				
	Generic List Block Type (31)				
	Generic List Block Length				
VDB Native Fingerprints 1	Operating System Fingerprint Block Type (130)*				
1 mgcrprmts 1	Operating System Fingerprint Block Length				
	Operating System VDB Fingerprint Data				
		Generic List B	lock Type (31)		
	Generic List Block Length				
VDB Native Fingerprints 2	Operating System Fingerprint Block Type (130)*				
1 mgerprints 2	Operating System Fingerprint Block Length				
Operating System VDB Fingerprint Data					
	Generic List Block Type (31)				
	Generic List Block Length				
User Fingerprints)*	
1 mgv1p1ms	Operating System Fingerprint Block Length				
Operating System User Fingerprint Data					
	Generic List Block Type (31)				
	Generic List Block Length				
Scan Fingerprints	Operating System Fingerprint Block Type (130)*				
g	Operating System Fingerprint Block Length				
Operating System Scan Fingerprint Data					
	Generic List Block Type (31)				
	Generic List Block Length				

Byte	0	1			2			3	
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 2	1 1 1 3 4 5	1 1 6 7	$\begin{array}{c cccc} 1 & 1 & 2 & 2 \\ 8 & 9 & 0 & 1 \end{array}$	2 2 3	2 2 4 5	$\begin{array}{c cccc} 2 & 2 & 2 & 2 \\ 6 & 7 & 8 & 9 \end{array}$	3 3 0 1
Application Fingerprints	Operating System Fingerprint Block Type (130)*								
Tingerprints	Operating System Fingerprint Block Length								
	Operating System Application Fingerprint Data								
	Generic List Block Type (31)								
	Generic List Block Length								
Conflict Fingerprints	Operating System Fingerprint Block Type (130)*								
81	Operating System Fingerprint Block Length								
	Operating System Conflict Fingerprint Data								
(TCP) Full Server Data	List Block Type (11)								
	List Block Length								
	(TCP) Full Server Data Blocks (104)*								
(UDP) Full Server Data	List Block Type (11)								
	List Block Length								
	(UDP) Full Server Data Blocks (104)*								
Network Protocol Data	List Block Type (11)								
	List Block Length								
	(Network) Protocol Data Blocks (4)*								
Transport Protocol Data	List Block Type (11)								
	List Block Length								
(Transport) Protocol Data Blocks (4)*									
MAC Address Data	List Block Type (11)								
	List Block Length								
	Host MAC Address Data Blocks (95)*								
	Last Seen								
	Host Type								
	Business	Criticality				VLA	N ID		

Byte	0	1	2	3	
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1	
	VLAN Type	VLAN Priority	Generic List B	lock Type (31)	
Host Client Data	Generic List Block Type, continued Generic List Block Length				
	Generic List Block Length, continued Full Host Client Application Data Blocks (112)*				
NetBIOS Name	String Block Type (0)				
T value	String Block Length				
	NetBIOS Name String				
Notes Data	String Block Type (0)				
	String Block Length				
Notes String					
(VDB) Host Vulns	Generic List Block Type (31)				
	Generic List Block Length				
	(VDB) Host Vulnerability Data Blocks (85)*				
3rd Pty/VDB) Host Vulns	Generic List Block Type (31)				
	Generic List Block Length				
	(Third Party/VDB) Host Vulnerability Data Blocks (85)*				
3rd Pty Scan Host Vulns	Generic List Block Type (31)				
	Generic List Block Length				
	(Third Party Scan) Host Vulnerability Data Blocks with Original Vuln IDs (85)*				
Attribute Value Data	List Block Type (11)				
	List Block Length				
	Attribute Value Data Blocks *				
	Mobile	Jailbroken	VLAN Presence		

The following table describes the components of the Full Host Profile for 5.1.1 record.

Table B-37 Full Host Profile Record 5.1.1 Fields

Field	Data Type	Description
IP Address	uint8[4]	IP address of the host, in IP address octets.
Hops	uint8	Number of network hops from the host to the device.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data derived from the existing fingerprints for the host. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.
Operating System Derived Fingerprint Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host derived from the existing fingerprints for the host. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data identified using a server fingerprint. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.
Operating System Fingerprint (Server Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host identified using a server fingerprint. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data identified using a client fingerprint. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.
Operating System Fingerprint (Client Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host identified using a client fingerprint. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data identified using a Cisco VDB fingerprint. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.
Operating System Fingerprint (VDB) Native Fingerprint 1) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host identified using the fingerprints in the Cisco vulnerability database (VDB). See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.

Table B-37 Full Host Profile Record 5.1.1 Fields (continued)

Field	Data Type	Description
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data identified using a Cisco VDB fingerprint. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.
Operating System Fingerprint (VDB) Native Fingerprint 2) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host identified using the fingerprints in the Cisco vulnerability database (VDB). See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data added by a user. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.
Operating System Fingerprint (User Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host added by a user. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data added by a vulnerability scanner. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.
Operating System Fingerprint (Scan Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host added by a vulnerability scanner. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data added by an application. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.
Operating System Fingerprint (Application Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host added by an application. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data selected through fingerprint conflict resolution. This value is always 31.

Table B-37 Full Host Profile Record 5.1.1 Fields (continued)

Field	Data Type	Description
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.
Operating System Fingerprint (Conflict Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host selected through fingerprint conflict resolution. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.
List Block Type	uint32	Initiates a List data block comprising Full Server data blocks conveying TCP service data. This value is always 11.
List Block Length	uint32	Number of bytes in the list. This number includes the eight bytes of the list block type and length fields, plus the length of all encapsulated Full Server data blocks.
(TCP) Full Server Data Blocks *	variable	List of Full Server data blocks conveying data about the TCP services on the host. See Full Host Server Data Block 4.10.0+, page 4-125 for a description of this data block.
List Block Type	uint32	Initiates a List data block comprising Full Server data blocks conveying UDP service data. This value is always 11.
List Block Length	uint32	Number of bytes in the list. This number includes the eight bytes of the list block type and length fields, plus the length of all encapsulated Full Server data blocks.
(UDP) Full Server Data Blocks *	variable	List of Full Server data blocks conveying data about the UDP sub-servers on the host. See Full Host Server Data Block 4.10.0+, page 4-125 for a description of this data block.
List Block Type	uint32	Initiates a List data block comprising Protocol data blocks conveying network protocol data. This value is always 11.
List Block Length	uint32	Number of bytes in the list. This number includes the eight bytes of the list block type and length fields, plus the length of all encapsulated Protocol data blocks.
(Network) Protocol Data Blocks *	variable	List of Protocol data blocks conveying data about the network protocols on the host. See Protocol Data Block, page 4-67 for a description of this data block.
List Block Type	uint32	Initiates a List data block comprising Protocol data blocks conveying transport protocol data. This value is always 11.
List Block Length	uint32	Number of bytes in the list. This number includes the eight bytes of the list block type and length fields, plus the length of all encapsulated Protocol data blocks.
(Transport) Protocol Data Blocks *	variable	List of Protocol data blocks conveying data about the transport protocols on the host. See Protocol Data Block, page 4-67 for a description of this data block.
List Block Type	uint32	Initiates a List data block containing Host MAC Address data blocks. This value is always 11.
List Block Length	uint32	Number of bytes in the list, including the list header and all encapsulated Host MAC Address data blocks.

Table B-37 Full Host Profile Record 5.1.1 Fields (continued)

Field	Data Type	Description		
Host MAC Address Data Blocks *	variable	List of Host MAC Address data blocks. See Host MAC Address 4.9+, page 4-105 for a description of this data block.		
Last Seen	uint32	UNIX timestamp that represents the last time the system detected host activity.		
Host Type	uint32	Indicates host type. Values include:		
		• 0 — Host		
		• 1 — Router		
		• 2 — Bridge		
		• 3 — NAT (network address translation device)		
		• 4 — LB (load balancer)		
Business Criticality	uint16	Indicates criticality of host to business.		
VLAN ID	uint16	VLAN identification number that indicates which VLAN the host is a member of.		
VLAN Type	uint8	Type of packet encapsulated in the VLAN tag.		
VLAN Priority	uint8	Priority value included in the VLAN tag.		
Generic List Block Type	uint32	Initiates a Generic List data block comprising Host Vulnerability data blocks conveying Client Application data. This value is always 31.		
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Client Application data blocks.		
Full Host Client Application Data Blocks *	variable	List of Client Application data blocks. See Full Host Client Application Data Block 5.0+, page 4-139 for a description of this data block.		
String Block Type	uint32	Initiates a String data block for the host NetBIOS name. This value is always 0.		
String Block Length	uint32	Number of bytes in the String data block, including eight bytes for the string block type and length fields, plus the number of bytes in the NetBIOS name string.		
NetBIOS Name	string	Host NetBIOS name string.		
String Block Type	uint32	Initiates a String data block for host notes. This value is always 0.		
String Block Length	uint32	Number of bytes in the notes String data block, including eight bytes for the string block type and length fields, plus the number of bytes in the notes string.		
Notes	string	Contains the contents of the Notes host attribute for the host.		
Generic List Block Type	uint32	Initiates a Generic List data block comprising Host Vulnerability data blocks conveying VDB vulnerability data. This value is always 31.		
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated data blocks.		

Table B-37 Full Host Profile Record 5.1.1 Fields (continued)

Field	Data Type	Description			
(VDB) Host Vulnerability Data Blocks *	variable	List of Host Vulnerability data blocks for vulnerabilities identified in the Cisco vulnerability database (VDB). See Host Vulnerability Data Block 4.9.0+, page 4-103 for a description of this data block.			
Generic List Block Type	uint32	Initiates a Generic List data block comprising Host Vulnerability data blocks conveying third-party scan vulnerability data. This value is always 31.			
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated data blocks.			
(Third Party/VDB) Host Vulnerability Data Blocks *	variable	Host Vulnerability data blocks sourced from a third party scanner and containing information about host vulnerabilities cataloged in the Cisco vulnerability database (VDB). See Host Vulnerability Data Block 4.9.0+, page 4-103 for a description of this data block.			
Generic List Block Type	uint32	Initiates a Generic List data block comprising Host Vulnerability data blocks conveying third party scan vulnerability data. This value is always 31.			
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated data blocks.			
(Third Party Scan) Host Vulnerability Data Blocks *	variable	Host Vulnerability data blocks sourced from a third party scanner. Note that the host vulnerability IDs for these data blocks are the third party scanner IDs, not Cisco-detected IDs. See Host Vulnerability Data Block 4.9.0+, page 4-103 for a description of this data block.			
List Block Type	uint32	Initiates a List data block comprising Attribute Value data blocks conveying attribute data. This value is always 11.			
List Block Length	uint32	Number of bytes in the List data block, including the list header and all encapsulated data blocks.			
Attribute Value Data Blocks *	variable	List of Attribute Value data blocks. See Attribute Value Data Block, page 4-73 for a description of the data blocks in this list.			
Mobile	uint8	A true-false flag indicating whether the operating system is running on a mobile device.			
Jailbroken	uint8	A true-false flag indicating whether the mobile device operating system is jailbroken.			
VLAN Presence	uint8	Indicates whether a VLAN is present:			
		• 0 — Yes • 1 — No			

Full Host Profile Data Block 5.2.x

The Full Host Profile data block for version 5.2.x contains a full set of data describing one host. It has the format shown in the graphic below and explained in the following table. Note that, except for List data blocks, the graphic does not show the fields of the encapsulated data blocks. These encapsulated data blocks are described separately in Understanding Discovery & Connection Data Structures, page 4-1. The Full Host Profile data block a block type value of 140. It supersedes the prior version, which has a block type of 135.



An asterisk (*) next to a block name in the following diagram indicates that multiple instances of the data block may occur.

Byte	0	1 2 3				
Bit	0 1 2 3 4 5 6 7 8 9 1 1 2 3 4 5 6 7 8 9 0 1 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1					
	Full Host Profile Data Block (140)					
	Data Block Length					
		Host ID				
		Host ID, continued				
		Host ID, continued				
		Host ID, continued				
IP Addresses		List Block Type (11)				
		List Block Length				
		IP Address Data Blocks (143)*				
	Hops Generic List Block Type (31)					
	Generic List Block Type, continued	Generic List Block Length				
OS Derived Fingerprints	Generic List Block Length, continued Operating System Fingerprint Block Type (130)*					
	OS Fingerprint Block Type (130)*, con't	Operating System Fingerprint Block Length				
	OS Fingerprint Block Length, con't	Operating System Derived Fingerprint Data				
		Generic List Block Type (31)				
		Generic List Block Length				
Server	Op	perating System Fingerprint Block Type (130)*				
Fingerprints	Operating System Fingerprint Block Length					
		Operating System Server Fingerprint Data				
		Generic List Block Type (31)				

Byte	0 1 2 3				
Bit	0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2				
	Generic List Block Length				
Client Fingerprints	Operating System Fingerprint Block Type (130)*				
Tingerprints	Operating System Fingerprint Block Length				
Operating System Client Fingerprint Data					
	Generic List Block Type (31)				
	Generic List Block Length				
VDB Native Fingerprints 1	Operating System Fingerprint Block Type (130)*				
1 mgorprims 1	Operating System Fingerprint Block Length				
	Operating System VDB Fingerprint Data				
	Generic List Block Type (31)				
	Generic List Block Length				
VDB Native Fingerprints 2	Operating System Fingerprint Block Type (130)*				
	Operating System Fingerprint Block Length				
	Operating System VDB Fingerprint Data				
	Generic List Block Type (31)				
	Generic List Block Length				
User Fingerprints	Operating System Fingerprint Block Type (130)*				
	Operating System Fingerprint Block Length				
	Operating System User Fingerprint Data				
	Generic List Block Type (31)				
	Generic List Block Length				
Scan Fingerprints	Operating System Fingerprint Block Type (130)*				
	Operating System Fingerprint Block Length				
	Operating System Scan Fingerprint Data				
	Generic List Block Type (31)				
	Generic List Block Length				

Byte	0	1	2	3		
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1		
Application Fingerprints	Operating System Fingerprint Block Type (130)*					
ringerprints	Operating System Fingerprint Block Length					
	OĮ	perating System Appli	cation Fingerprint Data	a		
		Generic List B	clock Type (31)			
		Generic List	Block Length			
Conflict Fingerprints	Ol	perating System Finge	rprint Block Type (130))*		
Tingerprints		Operating System Fin	gerprint Block Length			
	(Operating System Con	flict Fingerprint Data			
		Generic List B	clock Type (31)			
		Generic List	Block Length			
Mobile Fingerprints	Operating System Fingerprint Block Type (130)*					
1 mgerprims	Operating System Fingerprint Block Length					
	Operating System Mobile Fingerprint Data					
	Generic List Block Type (31)					
	Generic List Block Length					
IPv6 Server Fingerprints	O _l	perating System Finge	rprint Block Type (130))*		
8.1	Operating System Fingerprint Block Length					
	OĮ	perating System IPv6 S	Server Fingerprint Data	a		
		Generic List B	lock Type (31)			
		Generic List	Block Length			
Ipv6 Client Fingerprints	Operating System Fingerprint Block Type (130)*					
		Operating System Fingerprint Block Length				
	Oj	perating System Ipv6	Client Fingerprint Data	a		
		Generic List B	clock Type (31)			
		Generic List	Block Length			

Byte	0	1			2			3	
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 3	1 1 4 5	1 1 6 7	$\begin{array}{c cccc} 1 & 1 & 2 & 2 \\ 8 & 9 & 0 & 1 \end{array}$	$\begin{bmatrix} 2 & 2 \\ 2 & 3 \end{bmatrix}$	2 2 4 5	$ \begin{array}{c cccc} 2 & 2 & 2 & 2 \\ 6 & 7 & 8 & 9 \end{array} $	3 3 0 1
Ipv6 DHCP Fingerprints	Operating System Fingerprint Block Type (130)*								
Tingerprints	Operating System Fingerprint Block Length								
	Operating System IPv6 DHCP Fingerprint Data								
		Generic	List B	lock T	Гуре (31)				
		Generic	List	Block	Length				
User Agent Fingerprints	Ol	perating System	Finge	rprint	Block Type	(130)*		
i ingerprims		Operating Syste	m Fin	gerpri	nt Block Le	ength			
	Oj	perating System	User A	Agent	Fingerprint	t Data	•••		
(TCP) Full Server Data		List I	Block	Туре ((11)				
		List	Block	Leng	gth				
		(TCP) Full So	erver l	Data E	Blocks (104)*			
(UDP) Full Server Data	List Block Type (11)								
		Lis	t Bloc	k Len	gth				
	(UDP) Full Server Data Blocks (104)*								
Network Protocol Data	List Block Type (11)								
	List Block Length								
	(Network) Protocol Data Blocks (4)*								
Transport Protocol Data		List	Block	Туре	(11)				
		Lis	t Bloc	k Len	gth				
		(Transport) P)*			
MAC Address Data	List Block Type (11)								
	List Block Length								
		Host MAC A			Blocks (95	5)*			
			Last						
	D :	2.1.1	Host	Type		X / Y /			
	Business (Criticality				VLA	N ID		

Byte	0	1	2	3			
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1			
	VLAN Type	VLAN Priority	Generic List B	clock Type (31)			
Host Client Data	Generic List Block	Generic List Block Type, continued Generic List Block Length					
Duu	Generic List Block	Length, continued		olication Data Blocks 2)*			
NetBios Name		String Bloc	k Type (0)				
Name		String Blo	ck Length				
		NetBIOS Na	me String				
Notes Data		String Bloc	k Type (0)				
	String Block Length						
		Notes S	tring				
(VDB) Host Vulns	Generic List Block Type (31)						
	Generic List Block Length						
		(VDB) Host Vulnerabi	lity Data Blocks (85)*				
3rd Pty/VDB) Host Vulns	Generic List Block Type (31)						
	Generic List Block Length						
	(Third	Party/VDB) Host Vul	nerability Data Blocks	s (85)*			
3rd Pty Scan Host Vulns		Generic List B	lock Type (31)				
	Generic List Block Length						
	(Third Party Scan	ata Blocks with Origin	al Vuln IDs (85)*				
Attribute Value Data	List Block Type (11)						
		List Block Length					
		Attribute Value	Data Blocks *				
	Mobile	Jailbroken					

The following table describes the components of the Full Host Profile for 5.2.x record.

Table B-38 Full Host Profile Record 5.2.x Fields

Field	Data Type	Description		
Host ID	uint8[16]	Unique ID number of the host. This is a UUID.		
List Block Type	uint32	Initiates a List data block comprising IP address data blocks conveying TCP service data. This value is always 11.		
List Block Length	uint32	Number of bytes in the list. This number includes the eight bytes of the list block type and length fields, plus the length of all encapsulated IP address data blocks.		
IP Address	variable	IP addresses of the host and when each IP address was last seen. See Host IP Address Data Block, page 4-88 for a description of this data block.		
Hops	uint8	Number of network hops from the host to the device.		
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data derived from the existing fingerprints for the host. This value is always 31.		
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.		
Operating System Derived Fingerprint Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host derived from the existing fingerprints for the host. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.		
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data identified using a server fingerprint. This value is always 31.		
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.		
Operating System Fingerprint (Server Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host identified using a server fingerprint. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.		
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data identified using a client fingerprint. This value is always 31.		
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.		
Operating System Fingerprint (Client Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host identified using a client fingerprint. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.		
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data identified using a Cisco VDB fingerprint. This value is always 31.		

Table B-38 Full Host Profile Record 5.2.x Fields (continued)

Field	Data Type	Description
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.
Operating System Fingerprint (VDB) Native Fingerprint 1) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host identified using the fingerprints in the Cisco vulnerability database (VDB). See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data identified using a Cisco VDB fingerprint. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.
Operating System Fingerprint (VDB) Native Fingerprint 2) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host identified using the fingerprints in the Cisco vulnerability database (VDB). See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data added by a user. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.
Operating System Fingerprint (User Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host added by a user. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data added by a vulnerability scanner. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.
Operating System Fingerprint (Scan Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host added by a vulnerability scanner. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data added by an application. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.

Table B-38 Full Host Profile Record 5.2.x Fields (continued)

Field	Data Type	Description
Operating System Fingerprint (Application Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host added by an application. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data selected through fingerprint conflict resolution. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.
Operating System Fingerprint (Conflict Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host selected through fingerprint conflict resolution. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying mobile device fingerprint data. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.
Operating System Fingerprint (Mobile) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a mobile device host. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data identified using an IPv6 server fingerprint. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.
Operating System Fingerprint (IPv6 Server Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host identified using an IPv6 server fingerprint. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data identified using an IPv6 client fingerprint. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.

Table B-38 Full Host Profile Record 5.2.x Fields (continued)

Field	Data Type	Description
Operating System Fingerprint (IPv6 Client Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host identified using an IPv6 client fingerprint. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data identified using an IPv6 DHCP fingerprint. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.
Operating System Fingerprint (IPv6 DHCP) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host identified using an IPv6 DHCP fingerprint. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data identified using a user agent fingerprint. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.
Operating System Fingerprint (User Agent) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host identified using a user agent fingerprint. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.
List Block Type	uint32	Initiates a List data block comprising Full Server data blocks conveying TCP service data. This value is always 11.
List Block Length	uint32	Number of bytes in the list. This number includes the eight bytes of the list block type and length fields, plus the length of all encapsulated Full Server data blocks.
(TCP) Full Server Data Blocks *	variable	List of Full Server data blocks conveying data about the TCP services on the host. See Full Host Server Data Block 4.10.0+, page 4-125 for a description of this data block.
List Block Type	uint32	Initiates a List data block comprising Full Server data blocks conveying UDP service data. This value is always 11.
List Block Length	uint32	Number of bytes in the list. This number includes the eight bytes of the list block type and length fields, plus the length of all encapsulated Full Server data blocks.
(UDP) Full Server Data Blocks *	variable	List of Full Server data blocks conveying data about the UDP sub-servers on the host. See Full Host Server Data Block 4.10.0+, page 4-125 for a description of this data block.
List Block Type	uint32	Initiates a List data block comprising Protocol data blocks conveying network protocol data. This value is always 11.

Table B-38 Full Host Profile Record 5.2.x Fields (continued)

Field	Data Type	Description	
List Block Length	uint32	Number of bytes in the list. This number includes the eight bytes of the list block type and length fields, plus the length of all encapsulated Protocol data blocks.	
(Network) Protocol Data Blocks *	variable	List of Protocol data blocks conveying data about the network protocols on the host. See Protocol Data Block, page 4-67 for a description of this data block.	
List Block Type	uint32	Initiates a List data block comprising Protocol data blocks conveying transport protocol data. This value is always 11.	
List Block Length	uint32	Number of bytes in the list. This number includes the eight bytes of the list block type and length fields, plus the length of all encapsulated Protocol data blocks.	
(Transport) Protocol Data Blocks *	variable	List of Protocol data blocks conveying data about the transport protocols on the host. See Protocol Data Block, page 4-67 for a description of this data block.	
List Block Type	uint32	Initiates a List data block containing Host MAC Address data blocks. This value is always 11.	
List Block Length	uint32	Number of bytes in the list, including the list header and all encapsulated Host MAC Address data blocks.	
Host MAC Address Data Blocks *	variable	List of Host MAC Address data blocks. See Host MAC Address 4.9+, page 4-105 for a description of this data block.	
Last Seen	uint32	UNIX timestamp that represents the last time the system detected host activity.	
Host Type	uint32	Indicates host type. Values include:	
		• 0 — Host	
		• 1 — Router	
		• 2 — Bridge	
		• 3 — NAT (network address translation device)	
		• 4 — LB (load balancer)	
Business Criticality	uint16	Indicates criticality of host to business.	
VLAN ID	uint16	VLAN identification number that indicates which VLAN the host is a member of.	
VLAN Type	uint8	Type of packet encapsulated in the VLAN tag.	
VLAN Priority	uint8	Priority value included in the VLAN tag.	
Generic List Block Type	uint32	Initiates a Generic List data block comprising Host Vulnerability data blocks conveying Client Application data. This value is always 31.	
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Client Application data blocks.	

Table B-38 Full Host Profile Record 5.2.x Fields (continued)

Field	Data Type	Description
Full Host Client Application Data Blocks *	variable	List of Client Application data blocks. See Full Host Client Application Data Block 5.0+, page 4-139 for a description of this data block.
String Block Type	uint32	Initiates a String data block for the host NetBIOS name. This value is always 0.
String Block Length	uint32	Number of bytes in the String data block, including eight bytes for the string block type and length fields, plus the number of bytes in the NetBIOS name string.
NetBIOS Name	string	Host NetBIOS name string.
String Block Type	uint32	Initiates a String data block for host notes. This value is always 0.
String Block Length	uint32	Number of bytes in the notes String data block, including eight bytes for the string block type and length fields, plus the number of bytes in the notes string.
Notes	string	Contains the contents of the Notes host attribute for the host.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Host Vulnerability data blocks conveying VDB vulnerability data. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated data blocks.
(VDB) Host Vulnerability Data Blocks *	variable	List of Host Vulnerability data blocks for vulnerabilities identified in the Cisco vulnerability database (VDB). See Host Vulnerability Data Block 4.9.0+, page 4-103 for a description of this data block.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Host Vulnerability data blocks conveying third-party scan vulnerability data. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated data blocks.
(Third Party/VDB) Host Vulnerability Data Blocks *	variable	Host Vulnerability data blocks sourced from a third party scanner and containing information about host vulnerabilities cataloged in the Cisco vulnerability database (VDB). See Host Vulnerability Data Block 4.9.0+, page 4-103 for a description of this data block.
Generic List Block Type	uint32	Initiates a Generic List data block comprising Host Vulnerability data blocks conveying third party scan vulnerability data. This value is always 31.
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated data blocks.
(Third Party Scan) Host Vulnerability Data Blocks *	variable	Host Vulnerability data blocks sourced from a third party scanner. Note that the host vulnerability IDs for these data blocks are the third party scanner IDs, not Cisco-detected IDs. See Host Vulnerability Data Block 4.9.0+, page 4-103 for a description of this data block.
List Block Type	uint32	Initiates a List data block comprising Attribute Value data blocks conveying attribute data. This value is always 11.

Table B-38 Full Host Profile Record 5.2.x Fields (continued)

Field	Data Type	Description
List Block Length	uint32	Number of bytes in the List data block, including the list header and all encapsulated data blocks.
Attribute Value Data Blocks *	variable	List of Attribute Value data blocks. See Attribute Value Data Block, page 4-73 for a description of the data blocks in this list.
Mobile	uint8	A true-false flag indicating whether the operating system is running on a mobile device.
Jailbroken	uint8	A true-false flag indicating whether the mobile device operating system is jailbroken.

Host Profile Data Block for 5.1.x

The following diagram shows the format of a Host Profile data block. The data block also does not include a host criticality value, but does include a VLAN presence indicator. In addition, a data block can convey a NetBIOS name for the host. The Host Profile data block has a block type of 132.



An asterisk(*) next to a block type field in the following diagram indicates the message may contain zero or more instances of the series 1 data block.

Byte	0	1	2	3	
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1	
		Host Profile Blo	ock Type (132)		
		Host Profile I	Block Length		
		IP Ad	dress		
Server Fingerprints	Hops	Primary/Secondary	Generic List B	lock Type (31)	
1 ingerprints	Generic List Block	k Type, continued	Generic List Block Length		
	Generic List Block	Length, continued	Server Fingerpri	int Data Blocks*	
Client Fingerprints	Generic List Block Type (31)				
1 ingerprints	Generic List Block Length				
	Client Fingerprint Data Blocks*				
SMB Fingerprints	Generic List Block Type (31)				
ingerprints		Generic List I	Block Length		
		SMB Fingerprin	nt Data Blocks*		

Byte	0	1	2	3		
Bit	0 1 2 3 4 5 6 7					
DHCP Fingerprints						
ringerprints		Generic List	Block Length			
		DHCP Fingerpr	rint Data Blocks*			
Mobile Device		Generic List I	Block Type (31)			
Fingerprints		Generic List	Block Length			
		Mobile Device Fing	gerprint Data Blocks*			
TCP Server Block*		List Bloc	k Type (11)		List of TCP Servers	
Block		List Blo	ck Length		Servers	
		TCP Server	Data Blocks			
UDP Server Block*		List of UDP Servers				
BIOCK						
	UDP Server Data Blocks					
Network Protocol		List of Network Protocols				
Block*						
Transport Protocol		List Bloc	k Type (11)		List of Transport	
Block*		Protocols				
MAC Address Block*		List Block Type (11)				
	List Block Length				Addresses	
	Host MAC Address Data Blocks					
		Host Last Seen				
	Host Type					
	Mobile	Jailbroken	VLAN Presence	VLAN ID		

Byte	0	1	2	3	
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1	
Client App Data	VLAN ID, cont.	VLAN Type	VLAN Priority	Generic List Block Type (31)	List of Client Applications
	Generi	Generic List Block Type (31), cont. Generic List Block Length			
	Generic List Block Length, cont. Client Application Data Blocks				
NetBIOS Name					
Tallie					

The following table describes the fields of the host profile data block returned by version 5.1.x

Table B-39 Host Profile Data Block 5.1.x Fields

Field	Data Type	Description	
Host Profile Block Type	uint32	Initiates the Host Profile data block for 5.1.x. This value is always 132.	
Host Profile Block Length	uint32	Number of bytes in the Host Profile data block, including eight bytes for the host profile block type and length fields, plus the number of bytes included in the host profile data that follows.	
IP Address	uint8[4]	IP address of the host described in the profile, in IP address octets.	
Hops	uint8	Number of hops from the host to the device.	
Primary/ Secondary	uint8	Indicates whether the host is in the primary or secondary network of the device that detected it:	
		• 0 — Host is in the primary network.	
		• 1 — Host is in the secondary network.	
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data identified using a server fingerprint. This value is always 31.	
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.	
Operating System Fingerprint (Server Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host identified using a server fingerprint. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.	

Table B-39 Host Profile Data Block 5.1.x Fields (continued)

Field	Data Type	Description	
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data identified using a client fingerprint. This value is always 31.	
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.	
Operating System Fingerprint (Client Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host identified using a client fingerprint. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.	
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data identified using an SMB fingerprint. This value is always 31.	
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.	
Operating System Fingerprint (SMB Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host identified using an SMB fingerprint. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.	
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data identified using a DHCP fingerprint. This value is always 31.	
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.	
Operating System Fingerprint (DHCP Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host identified using a DHCP fingerprint. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.	
Generic List Block Type	uint32	Initiates a Generic List data block comprising Operating System Fingerprint data blocks conveying fingerprint data identified using a DHCP fingerprint. This value is always 31.	
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated Operating System Fingerprint data blocks.	

Table B-39 Host Profile Data Block 5.1.x Fields (continued)

Field	Data Type	Description	
Operating System Fingerprint (Mobile Device Fingerprint) Data Blocks *	variable	Operating System Fingerprint data blocks containing information about the operating system on a host identified using a mobile device fingerprint. See Operating System Fingerprint Data Block 5.1+, page 4-144 for a description of this data block.	
List Block Type	uint32	Initiates a List data block comprising Server data blocks conveying TCP server data. This value is always 11.	
List Block Length	uint32	Number of bytes in the list. This number includes the eight bytes of the list block type and length fields, plus all encapsulated Server data blocks.	
		This field is followed by zero or more Server data blocks.	
TCP Server Data Blocks	variable	Host server data blocks describing a TCP server (as documented for earlier versions of the product).	
List Block Type	uint32	Initiates a List data block comprising Server data blocks conveying UDP server data. This value is always 11.	
List Block Length	uint32	Number of bytes in the list. This number includes the eight bytes of the list block type and length fields, plus all encapsulated Server data blocks.	
		This field is followed by zero or more Server data blocks.	
UDP Server Data Blocks	uint32	Host server data blocks describing a UDP server (as documented for earlier versions of the product).	
List Block Type	uint32	Initiates a List data block comprising Protocol data blocks conveying network protocol data. This value is always 11.	
List Block Length	uint32	Number of bytes in the list. This number includes the eight bytes of the list block type and length fields, plus all encapsulated Protocol data blocks.	
		This field is followed by zero or more Protocol data blocks.	
Network Protocol Data Blocks	uint32	Protocol data blocks describing a network protocol. See Protocol Data Block, page 4-67 for a description of this data block.	
List Block Type	uint32	Initiates a List data block comprising Protocol data blocks conveying transport protocol data. This value is always 11.	
List Block Length	uint32	Number of bytes in the list. This number includes the eight bytes of the list block type and length fields, plus all encapsulated Protocol data blocks.	
		This field is followed by zero or more transport protocol data blocks.	
Transport Protocol Data Blocks	uint32	Protocol data blocks describing a transport protocol. See Protocol Data Block, page 4-67 for a description of this data block.	
List Block Type	uint32	Initiates a List data block comprising MAC Address data blocks. This value is always 11.	
List Block Length	uint32	Number of bytes in the list, including the list header and all encapsulated MAC Address data blocks.	

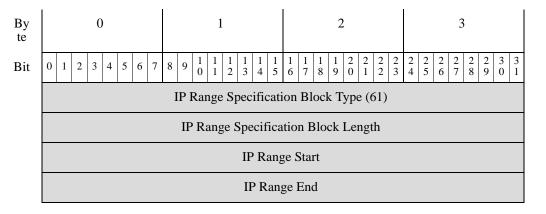
Table B-39 Host Profile Data Block 5.1.x Fields (continued)

Field	Data Type	Description		
Host MAC Address Data Blocks	uint32	Host MAC Address data blocks describing a host MAC address. See Host MAC Address 4.9+, page 4-105 for a description of this data block.		
Host Last Seen	uint32	UNIX timestamp that represents the last time the system detected host activity.		
Host Type	uint32	Indicates the host type. The following values may appear:		
		• 0 — Host		
		• 1 — Router		
		• 2 — Bridge		
		• 3 — NAT device		
		• 4 — LB (load balancer)		
Mobile	uint8	True-false flag indicating whether the host is a mobile device.		
Jailbroken	uint8	True-false flag indicating whether the host is a mobile device that is also jailbroken.		
VLAN Presence	uint8	Indicates whether a VLAN is present:		
		• 0 — Yes		
		• 1 — No		
VLAN ID	uint16	VLAN identification number that indicates which VLAN the host is a member of.		
VLAN Type	uint8	Type of packet encapsulated in the VLAN tag.		
VLAN Priority	uint8	Priority value included in the VLAN tag.		
Generic List Block Type	uint32	Initiates a Generic List data block comprising Client Application data blocks conveying client application data. This value is always 31.		
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated client application data blocks.		
Client Application Data Blocks	uint32	Client application data blocks describing a client application. See Full Host Client Application Data Block 5.0+, page 4-139 for a description of this data block.		
String Block Type	uint32	Initiates a string data block for the NetBIOS name. This value is set to 0 to indicate string data.		
String Block Length	uint32	Indicates the number of bytes in the NetBIOS name data block, including eight bytes for the string block type and length, plus the number of bytes in the NetBIOS name.		
NetBIOS String Data	Variable	Contains the NetBIOS name of the host described in the host profile.		

IP Range Specification Data Block for 5.0 - 5.1.1.x

The IP Range Specification data block conveys a range of IP addresses. IP Range Specification data blocks are used in User Protocol, User Client Application, Address Specification, User Product, User Server, User Hosts, User Vulnerability, User Criticality, and User Attribute Value data blocks. The IP Range Specification data block has a block type of 61.

The following diagram shows the format of the IP Range Specification data block:



The following table describes the components of the IP Range Specification data block.

Table B-40 IP Range Specification Data Block Fields

Field	Data Type	Description
IP Range Specification Block Type	uint32	Initiates a IP Range Specification data block. This value is always 61.
IP Range Specification Block Length	uint32	Total number of bytes in the IP Range Specification data block, including eight bytes for the IP Range Specification block type and length fields, plus the number of bytes of IP range specification data that follows.
IP Range Specification Start	uint32	The starting IP address for the IP address range.
IP Range Specification End	uint32	The ending IP address for the IP address range.