

# **Understanding Legacy Data Structures**

This appendix contains information about data structures supported by eStreamer at previous versions of Secure Firewall 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 Secure Firewall 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-68
- Legacy Discovery Data Structures, page B-121
- Legacy Connection Data Structures, page B-158
- Legacy File Event Data Structures, page B-290
- Legacy Correlation Event Data Structures, page B-331
- Legacy Host Data Structures, page B-346

# **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 Event Record 5.4.x, page B-36
- Intrusion Event Record 6.x, page B-44

- Intrusion Event Record 7.0, page B-53
- Intrusion Impact Alert Data, page B-62
- Intrusion Event Extra Data Record, page B-65
- Intrusion Event Extra Data Metadata, page B-66

# 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 2-13 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				Ì																					
Bit	0	1	2	3	4	5	6	7	8	9	1 0	1	1 2	2	1 3	1		1	1	1	1	18	1 9		2	2	2 2	3	2	2 4	2 5	2	2	2 7	2 8	2 9	3	3	3
					Не	ead	ler	Ve	rsi	on	(1	)													N	1e:	ssa	ıge	e T	Гу	pe	(4	1)						
	Message Length																																						
	Netmap ID Record Type (207)																																						
	Record Length																																						
	eStreamer Server Timestamp (in events, only if bit 23 is set)																																						
	Reserved for Future Use (in events, only if bit 23 is set)																																						
	Device ID																																						
																F	Eve	en	t I	D																			
															Е	ve	ent	S	Sec	O	nd	l																	
													]	Ev	/er	nt	M	ic	ro	se	ecc	on	d																
													Rı	ıle	e I	D	(5	iį	gna	atı	ure	e I	D,	)															
															G	ìе	ne	ra	to	r I	D																		
															R	ul	e l	Re	evi	si	or	ı																	
														(	Cla	ıss	sif	ica	ati	or	n I	D																	
	Priority ID																																						
													S	O	uro	ce	IF	V	4 /	A	dd	re	SS																

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	$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$				
		Destination II	Pv4 Address					
	Source	e Port	Destinati	ion Port				
	IP Protocol ID	Impact Flags	Impact Blocked					
	MPLS Label							
	VLAN ID Pad							
	Policy UUID							
	Policy UUID, continued							
		Policy UUID	), continued					
	Policy UUID, continued							
	User ID							
	Web Application ID							
	Client Application ID							
		Application l	Protocol ID					
		Access Contr	rol Rule ID					
		Access Control	Policy UUID					
		Access Control Polic	ey UUID, continued					
		Access Control Polic	ey UUID, continued					
		Access Control Polic						
		Interface Ing						
		Interface Ingress I						
		Interface Ingress U						
		Interface Ingress U						
		Interface Eg						
		Interface Egress U						
		Interface Egress U	JUID, continued					

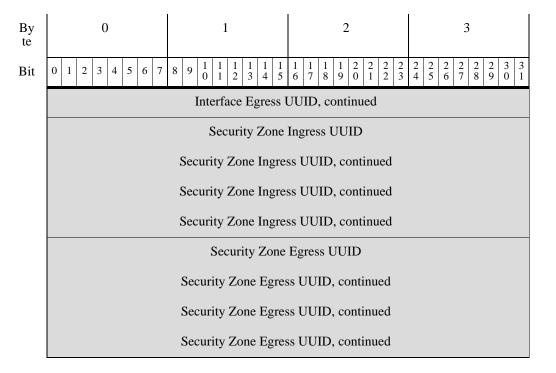


Table B-1 Intrusion Event (IPv4) Record Fields

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 3-33 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 uint32 Microsecond		Microsecond (one millionth of a second) increment of the timestamp of the event's detection.		
Rule ID uint32 (Signature ID)		Rule identification number that corresponds with the event.		
Generator ID	uint32	Identification number of the Secure Firewall 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.		

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

Field	Data Type	Description
Source Port	uint16	The source port number if the event protocol type is TCP or UDP.
<b>Destination Port</b>	uint16	The destination port number if the event protocol type is TCP or UDP.
IP Protocol Number	uint8	IANA-specified protocol number. For example:  • 0 — IP
		7015
		• 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 Secure Firewall 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 2-13 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 Vo	ersion (1)	Message	Type (4)					
		Message	Length						
	Netma	ap ID	Record T	ype (208)					
		Record	Length						
	eStreamer Server Timestamp (in events, only if bit 23 is set)								
	Reserved for Future Use (in events, only if bit 23 is set)								
	Device ID								
	Event ID								
	Event Second								
	Event Microsecond								
		Rule ID (Sig	gnature ID)						
		Genera	tor ID						
		Rule Re	evision						
		Classifica	ation ID						
		Priorit	y ID						
		Source IPv	6 Address						
		Source IPv6 Add	lress, continued						
		Source IPv6 Add	lress, continued						
		Source IPv6 Add	lress, continued						
		Destination II	Pv6 Address						
		Destination IPv6 A	ddress, continued						
		Destination IPv6 A	ddress, 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					
		Destination IPv6 A	Address, continued						
	Source Port/	ІСМР Туре	Destination Po	rt/ICMP Code					
	IP Protocol ID	Impact Flags	Impact	Blocked					
	MPLS Label								
	VLAN ID Pad								
	Policy UUID								
	Policy UUID, continued								
	Policy UUID, continued								
	Policy UUID, continued								
	User ID								
	Web Application ID								
	Client Application ID								
	Application Protocol ID								
		Access Cont	trol 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 V	UUID, continued						
		Interface Egress V	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 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 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 Egress UUID, continued							
	Security Zone Egress UUID, continued							
	Security Zone Egress 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 3-33 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 uint32 Microsecond		Microsecond (one millionth of a second) increment of the timestamp of the event's detection.			
Rule ID uint32 (Signature ID)		Rule identification number that corresponds with the event.			
Generator ID	uint32	Identification number of the Secure Firewall 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	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.																
	syste • 0x10	• 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 Secure Firewall 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-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 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							
	Netmap ID 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 Length							
	Device ID							
		Even	t ID					
		Event S	Second					
		Event Mic	rosecond					
		Rule ID (Sig	gnature ID)					
		Genera	tor ID					
		Rule Re	evision					
		Classific	ation ID					
		Priori	ty ID					

Byte			0				Ī		1	l				2 3											
Bit	0 1	2	3 4	5	6	5 7	8	9 1 0	1	1 2	1 3	1 4		1 1 5 7		1 2 9 0	2	2 2 2	2	2	2 2 5 6	2 7	2 8 9	3	3
		Source IP Address  Source IP Address, continued  Source IP Address, continued  Source IP Address, continued																							
														P A											
																ntin									
																ntini									
								De	StII	ıaı.	.1011	IP	Auc	ness	i, co	ntin	iea								
			Sour	ce l	Po	ort o	r IO	СМР	Туј	pe					De	stina	tior	Po	rt c	or	ICM	РС	ode		
	II	P Pr	otoco	ol II	D			Imp	act	t F	lags	8			In	прас	t				В	loc	ked		
											N	ΛPI	LS I	Labe	1										
					V	'LA	N I	D										P	ad						
											P	oli	cy L	UII	)										
									P	oli	icy	UU	ЛD,	con	tinu	ed									
											•			con											
									P	oli	icy			con	tinu	ed									
													ser												
														atio											
														catio											
														roto											
														ol R											
																UII		ad							
								Acces					Ī												
								Acces Acces					Ī												
							F	1000									unu	cu							
									1	.1116	erra	ce	mgi	ess	UUI	D									

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 2 2 2 2 2 2 2									
		Interface Ingress UUID, continued								
	Interface Ingress UUID, continued									
	Interface Ingress UUID, continued									
	Interface Egress UUID									
		Interface Egress U	JUID, continued							
		Interface Egress UUID, 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 Egres	ss 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
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, 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 3-33 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 Secure Firewall 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	uint8	IANA-specified protocol number. For example:
Number		• 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 Secure Firewall 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-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	e 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 2 2 6 7 8 9 0 1 2 3 4 5	2 2 2 2 3 3 6 7 8 9 0 1					
	Header Version (1) Message Type (4)								
		Message	Length						
	Netmap ID Record Type (400)								
		Record I	Length						
	eStrean	ner Server Timestamp (i	n events, only if bit 23 is set	t)					
	Rese	rved for Future Use (in	events, only if bit 23 is set)						
		Block Type (41)							
	Block Length  Device ID								
		Event	i ID						
		Event S	econd						
		Event Mic	rosecond						
		Rule ID (Sig	nature ID)						
		Generat	tor ID						
		Rule Re	vision						
		Classifica	ation ID						
		Priorit	y ID						
		Source IP	Address						
		Source IP Addre							
		Source IP Addre							
		Source IP Addre	ess, continued						

Byte	0			1	Ĺ			2 3									
Bit	0 1 2 3 4 5 6	8	$\begin{vmatrix} 9 & 1 \\ 0 & \end{vmatrix}$	1 1	1 1 2 3		1 1 5 6	1 7	1 1 8 9	2 0	2 2	2 3	2 4	2 2 6	2 2 2	2 9	3 3 0 1
				]	Desti	nati	on IF	Ac	ldress	S							
		Destination IP Address, continued															
	Destination IP Address, continued  Destination IP Address, continued																
	Source Port or ICMP Type Destination Port or ICMP Code																
	IP Protocol ID Impact Flags Impact Blocked																
		MPLS Label															
	VLAN ID Pad																
		Policy UUID Policy UUID, continued															
	Policy UUID, continued																
				P	olicy				tinue	d							
							ser I										
							plica										
									on ID								
									col II								
									ule II								
									ey UU			.1					
			Access Access				·										
			Access				·										
									UUIE		inuc	u 					
			Inte				_		o con		ıed						
						_			, con								
						_			, con								
			21110						JUID								
							_5.0	JJ <b>(</b>									

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 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	Interface Egress UUID, continued								
	Interface Egress UUID, continued									
	Interface Egress UUID, continued									
	Security Zone	Security Zone Ingress UUID								
	Security Zone Ingress UUID, continued									
	Security Zone Ingress UUID, continued									
	Security Zone Ingr	ess UUID, continued								
	Security Zon	e Egress UUID								
	Security Zone Egro	ess UUID, continued								
	Security Zone Egro	ess UUID, continued								
	Security Zone Egro	ess UUID, continued								
	Connection	Connection Timestamp								
	Connection Instance ID	Connectio	n Counter							
	Source Country	Destinatio	n Country							
	IOC Number									

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, 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 3-33 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 Secure Firewall 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 Secure Firewall 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
		• 2 — Would be blocked (but not permitted by configuration)

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.

By te	0	1	2	3		
Bit	0 1 2 3 4 5 6 7	0 1 2 3 4 3	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		
	Header V	ersion (1)	Message	Type (4)		
	Message Length					
	Netmap ID Record Type (400)					
		Record 1	Length			
	eStream	ner Server Timestamp (	in events, only if bit 23	3 is set)		
	Resei	rved for Future Use (in	events, only if bit 23 is	s set)		
		Block Ty	vpe (25)			
		Block I	ength			
	Device ID					
	Event ID					
	Event Second					
		Event Mic	rosecond			
		Rule ID (Sig	gnature ID)			
		Genera	tor ID			
		Rule Re	vision			
		Classifica	ation ID			
	Priority ID					
		Source IP	Address			
		Source IP Addr	ess, continued			
		Source IP Addr	ess, continued			
		Source IP Addr	ess, 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 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 Ac	ldress, continued			
		Destination IP Ac	ldress, continued			
	Source Port/	ICMP Type	Destination Po	rt/ICMP Code		
	IP Protocol ID	Impact Flags	Impact	Blocked		
		MPLS	Label			
	VLA	N ID	Pa	nd		
		Policy	UUID			
		Policy UUII	), continued			
		Policy UUII	O, continued			
	Policy UUID, continued					
	User ID					
	Web Application ID					
	Client Application ID					
	Application Protocol ID					
		Access Cont	trol Rule ID			
		Access Control	l Policy UUID			
		Access Control Policy UUID, continued				
		Access Control Police	cy UUID, continued			
	Access Control Policy 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 4	1 1 1 1 5 6 7 8	1 2 2 2 2 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1
		Interface I	gress UUI	D	
		Interface Egress	UUID, con	ntinued	
		Interface Egress	UUID, con	ntinued	
		Interface Egress	UUID, con	ntinued	
		Security Zone	Ingress U	UID	
	Security Zone Ingress UUID, continued				
	Security Zone Ingress UUID, continued				
	Security Zone Ingress UUID, continued				
	Security Zone Egress UUID				
		Security Zone Egress UUID, continued			
	Security Zone Egress UUID, continued				
	Security Zone Egress UUID, continued				
		Connection	n Timestam	ıp	
	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 3-33 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 Secure Firewall 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 Secure Firewall 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 5 6 7 8 9 1 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 2 2 2 2 2 2 2 2 3 3 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1					
	Header Version (1)	Message Type (4)					
	Message Length						
	Netmap ID	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 T	ype (42)					
	Block l	Length					
	Devid	ee ID					
	Even	ıt ID					
	Event S	Event Second					
	Event Microsecond						
	Rule ID (Signature ID)						
	Generator ID						
	Rule Revision						
	Classification ID						
	Priori	ty ID					
	Source IP	Address					
	Source IP Addi						
	Source IP Address, continued						
	Source IP Address, continued						
	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	$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	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
	Source Port	Source Port or ICMP Type			or ICMP Code
	IP Protocol ID Impact Flags			Impact	Blocked
	MPL			Label	
	VL	AN ID		Pa	ıd
			Policy	UUID	
		I	Policy UUII	O, continued	
		I	Policy UUII	O, continued	
		I	Policy UUII	O, continued	
			Use	r ID	
			Web Appl	ication ID	
	Client Application ID				
	Application Protocol ID				
	Access Control Rule ID				
	Access Control Policy UUID				
	Access Control Policy UUID, continued				
	Access Control Policy UUID, continued				
		Access (	Control Poli	cy UUID, continued	
				gress UUID	
		Interf	ace Ingress	UUID, continued	
		Interf	ace Ingress	UUID, continued	
		Interf	ace Ingress	UUID, continued	
				gress UUID	
				UUID, continued	
		Interface Egress UUID, continued			
		Interf	ace Egress	UUID, continued	
		Sec	curity Zone	Ingress UUID	

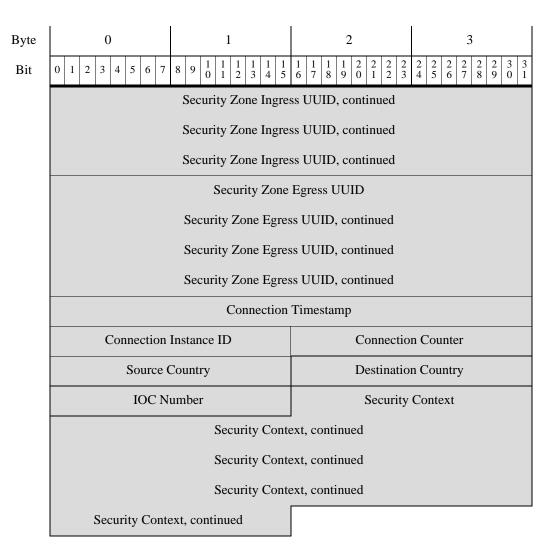


Table B-6 Intrusion Event Record 5.3.1 Fields

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 3-33 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 Secure Firewall 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	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 Secure Firewall 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 Event Record 5.4.x**

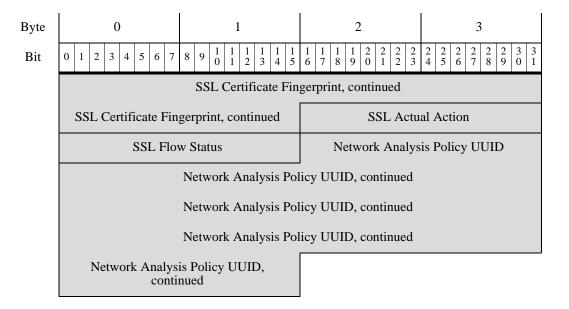
The fields in the intrusion event record are shaded in the following graphic. The record type is 400 and the block type is 45 in the series 2 set of data blocks. It supersedes block type 42, and is superseded by block type 60. Fields for SSL support and Network Analysis Policy have been added.

You can request 5.4.x intrusion events from eStreamer only by extended request, for which you request event type code 12 and version code 8 in the Stream Request message (see Submitting Extended Requests, page 2-4 for information about submitting extended requests).

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 Ve	ersion (1)	Message	Type (4)			
	Message Length						
	Netma	ap ID	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 (45)						
	Block Length						
	Device ID						
	Event ID						
	Event Second						
	Event Microsecond						
	Rule ID (Signature ID)						
	Generator ID						
	Rule Revision						
	Classification ID						
	Priority ID						

Byte		0						1	1						2						3						
Bit	0 1 2	3 4	1 5	6	7	8	9 1 0	1	1 2		1 4	1 1		1 8	1	2	2	2	2 3	2 4	2 2	2	2 2 7 8	2 9	3 3 0 1		
									,	Sou	rce	IP A	Addı	ress	3												
							S	Sou	ırc	e IF	P A	ddre	ss, c	ont	inu	ıed											
												ddre															
							,	Sou	irc	e IF	P A	ddre	ss, c	ont	inu	ıed											
								]	De	estin	ati	on I	P Ac	ddre	ess												
	Destination IP Address, continued																										
	Destination IP Address, continued																										
	Destination IP Address, continued																										
	Source Port or ICMP Type Destination Port or ICMP Code												de														
	IP Pı	rotoc	ol I	D			Imp	act	t F	lags	s			I	mp	act					]	B	lock	ed			
	MPLS Label																										
				V	LA	N I	D												Pa	ıd							
	Policy UUID																										
								P	Pol	licy	UU	ЛD,	con	tin	ued	l											
								P	ol	licy	UU	ЛD,	con	tin	ued	l											
								P	Pol	licy	UU	JID,	con	tin	ued	l											
											U	ser ]	D														
									V	Veb	Ap	plic	atio	n II	)												
									Cl	lien	t A	ppli	catio	on I	D												
								A	Ap <sub>1</sub>	plic	atio	on P	roto	col	ID	)											
								A	Ac	cess	s C	ontr	ol R	ule	ID												
								Aco	ces	ss C	ont	rol l	Poli	ey l	JU	ΙD											
							Acces																				
							Acces																				
						A	Acces										inu	ed									
								I	[nt	erfa	nce	Ingr	ess	UU	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 2 2 2 2 2 2 2 2 3 3 3 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 Eg	gress UUID										
	Interface Egress UUID, continued											
	Interface Egress UUID, 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											
	Security Zone Egres											
	Security Zone Egres Security Zone Egres											
	Connection											
	Connection Instance ID	Connection Counter										
	Source Country	Destination Country										
	IOC Number	Security Context										
	Security Conte	ext, continued										
	Security Conte	ext, continued										
	Security Conte	ext, continued										
	Security Context, continued	SSL Certificate Fingerprint										
	SSL Certificate Fin	gerprint, continued										
	SSL Certificate Fin	gerprint, continued										
	SSL Certificate Fin	gerprint, continued										



The following table describes each intrusion event record data field.

Table B-7 Intrusion Event Record 5.4.x Fields

Field	Data Type	Description
Block Type	unint32	Initiates an Intrusion Event data block. This value is always 45.
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 3-33 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 Secure Firewall 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.

Table B-7 Intrusion Event Record 5.4.x Fields (continued)

Field	Data Type	Description
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	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 Secure Firewall System web interface.
		• 0x40 (bit 6) — The rule that generated this event contains rule metadata setting the impact flag to red. The source or destination host is potentially compromised by a virus, trojan, or other piece of malicious software.
		• 0x80 (bit 7) — There is a vulnerability mapped to the client detected in the event. (version 5.0+ only)
		The following impact level values map to specific priorities on the Defense Center. An x indicates the value can be 0 or 1:
		• gray (0, unknown): 00x00000
		• red (1, vulnerable): xxxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx (version 5.0+ only)
		• orange (2, potentially vulnerable): 00x0011x
		• yellow (3, currently not vulnerable): 00x0001x
		• blue (4, unknown target): 00x00001

Table B-7 Intrusion Event Record 5.4.x 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 — Gray (unknown impact)
Blocked	uint8	Value indicating whether the event was blocked.
		• 0 — Not blocked
		• 1 — Blocked
		• 2 — Would be blocked (but not permitted by configuration)
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.

Table B-7 Intrusion Event Record 5.4.x Fields (continued)

Field	Data Type	Description						
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.						
SSL Certificate Fingerprint	uint8[20]	SHA1 hash of the SSL Server certificate.						
SSL Actual Action	uint16	The action performed on the connection based on the SSL Rule. This may differ from the expected action, as the action as specified in the rule may be impossible. Possible values include:						
		• 0 — 'Unknown'						
		• 1 — 'Do Not Decrypt'						
		• 2 — 'Block'						
		• 3 — 'Block With Reset'						
		• 4 — 'Decrypt (Known Key)'						
		• 5 — 'Decrypt (Replace Key)'						
		• 6 — 'Decrypt (Resign)'						

Table B-7 Intrusion Event Record 5.4.x Fields (continued)

Field	Data Type	Description
SSL Flow Status	uint16	Status of the SSL Flow. These values describe the reason behind
		the action taken or the error message seen. Possible values
		include:
		• 0 — 'Unknown'
		• 1 — 'No Match'
		• 2 — 'Success'
		• 3 — 'Uncached Session'
		• 4 — 'Unknown Cipher Suite'
		• 5 — 'Unsupported Cipher Suite'
		• 6 — 'Unsupported SSL Version'
		• 7 — 'SSL Compression Used'
		8 — 'Session Undecryptable in Passive Mode'
		• 9 — 'Handshake Error'
		• 10 — 'Decryption Error'
		• 11 — 'Pending Server Name Category Lookup'
		• 12 — 'Pending Common Name Category Lookup'
		• 13 — 'Internal Error'
		• 14 — 'Network Parameters Unavailable'
		• 15 — 'Invalid Server Certificate Handle'
		• 16 — 'Server Certificate Fingerprint Unavailable'
		• 17 — 'Cannot Cache Subject DN'
		• 18 — 'Cannot Cache Issuer DN'
		• 19 — 'Unknown SSL Version'
		• 20 — 'External Certificate List Unavailable'
		• 21 — 'External Certificate Fingerprint Unavailable'
		• 22 — 'Internal Certificate List Invalid'
		• 23 — 'Internal Certificate List Unavailable'
		• 24 — 'Internal Certificate Unavailable'
		• 25 — 'Internal Certificate Fingerprint Unavailable'
		• 26 — 'Server Certificate Validation Unavailable'
		• 27 — 'Server Certificate Validation Failure'
		• 28 — 'Invalid Action'
Network Analysis Policy UUID	uint8[16]	The UUID of the Network Analysis Policy that created the intrusion event.

#### **Intrusion Event Record 6.x**

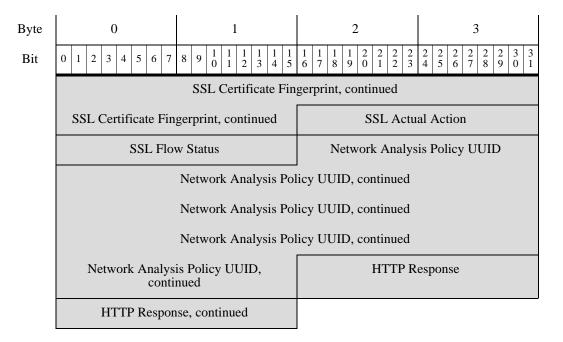
The fields in the intrusion event record are shaded in the following graphic. The record type is 400 and the block type is 60 in the series 2 set of data blocks. It supersedes block type 45, and is superseded by block type 81 in 7.0. An HTTP Response field has been added.

You can request 6.x intrusion events from eStreamer only by extended request, for which you request event type code 12 and version code 9 in the Stream Request message (see Submitting Extended Requests, page 2-4 for information about submitting extended requests).

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										
	Netma	np ID	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 (60)												
		Block I	Length										
		Devic	ee ID										
		Even	t ID										
		Event S	Second										
		Event Mic	crosecond										
		Rule ID (Sig	gnature ID)										
		Genera	tor ID										
		Rule Re	evision										
		Classific	ation ID										
		Priori	ty ID										

Byte		0			Ī				1							2					3							
Bit	0 1 2	3 4	5	6	7	8		1 1		1 1 2 3			1 1 5 6	1 7	1 8	1 9	2	2	2 2	2 3	2 4	2 2 6		2 2 2 7 8			3	
										So	urce	e I	IP A	ddı	ress	S												
													dres															
													dres															
								Sot	ır	ce I	PΑ	a	dres	ss, c	on	tinu	ıec	l										
									D	esti	nati	io	n IP	Ac	ldr	ess												
		Destination IP Address, continued																										
		Destination IP Address, continued  Destination IP Address, continued																										
		Destination IP Address, continued																										
	Source Port or ICMP Type Destination Port or ICMP Code																											
	IP Pı	rotoco	ol II	D			In	pac	t ]	Flag	gs				I	[mp	acı	t				I	310	ock	ed			
	MPLS Label																											
	VLAN ID Pad																											
											Poli	ic	y U	UII	)													
								I	Po	olicy	y UI	U]	ID,	con	tin	ued	l											
								I	Po	olicy	y UI	U]	ID,	con	tin	ued	l											
								I	Po	olicy	y UI	U]	ID,	con	tin	ued	l											
											ι	Js	er I	D —														
													plica															
												_	plic															
									_				n Pr															
													ntro															
													ol P															
													licy 															
													licy															
						I	Acce						licy					inu	ed									
									In	iterf	ace	I	ngre	ess	UU	JID												

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 3 3 4 5 6 7 8 9 0 1									
	Interface Ingress	UUID, continued										
	Interface Ingress	UUID, continued										
	Interface Ingress	UUID, continued										
	Interface Eg	ress UUID										
	Interface Egress	JUID, continued										
	Interface Egress	JUID, continued										
	Interface Egress UUID, continued											
	Security Zone Ingress UUID											
	Security Zone Ingress UUID, continued											
	Security Zone Ingre											
	Security Zone Ingre											
	Security Zone											
	Security Zone Egree											
	Security Zone Egree											
	Security Zone Egree											
	Connection  Connection Instance ID		n Countain									
	Source Country	Connection										
	IOC Number	Security										
	Security Conto	· ·	Context									
	Security Conto											
	Security Conto											
	Security Context, continued	SSL Certificat	te Fingerprint									
	SSL Certificate Fin											
	SSL Certificate Fin	gerprint, continued										
	SSL Certificate Fin	gerprint, continued										



The following table describes each intrusion event record data field.

Table B-8 Intrusion Event Record 6.x Fields

Field	Data Type	Description
Block Type	unint32	Initiates an Intrusion Event data block. This value is always 60.
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 3-33 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 Secure Firewall 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.

Table B-8 Intrusion Event Record 6.x Fields (continued)

Field	Data Type	Description
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 ID	uint8	IANA-specified protocol number. For example:  • 0 — IP  • 1 — ICMP  • 6 — TCP  • 17 — UDP

Table B-8 Intrusion Event Record 6.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 Secure Firewall 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 Management Center. An x indicates the value can be 0 or 1:
		• gray (0, unknown): 00x00000
		• red (1, vulnerable): xxxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx (version 5.0+ only)
		• orange (2, potentially vulnerable): 00x0011x
		• yellow (3, currently not vulnerable): 00x0001x
		• blue (4, unknown target): 00x00001
Impact	uint8	Impact flag value of the event. Values are:
		• 1 — Red (vulnerable)
		• 2 — Orange (potentially vulnerable)
		• 3 — Yellow (currently not vulnerable)
		• 4 — Blue (unknown target)
		• 5 — Gray (unknown impact)
Blocked	uint8	Value indicating whether the event was blocked.
		• 0 — Not blocked
		• 1 — Blocked
		• 2 — Would be blocked (but not permitted by configuration)

Table B-8 Intrusion Event Record 6.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.				
Interface Ingress UUID	uint8[16]	An interface ID number that acts as a unique identifier for the ingress interface.				
Interface Egress UUID	uint8[16]	An interface ID number that acts as a unique identifier for the egress interface.				
Security Zone Ingress UUID	uint8[16]	A zone ID number that acts as a unique identifier for the ingress security zone.				
Security Zone Egress 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.				
SSL Certificate Fingerprint	uint8[20]	SHA1 hash of the SSL Server certificate.				

Table B-8 Intrusion Event Record 6.x Fields (continued)

Field	Data Type	Description
SSL Actual Action	uint16	The action performed on the connection based on the SSL Rule. This may differ from the expected action, as the action as specified in the rule may be impossible. Possible values include:
		• 0 — 'Unknown'
<ul> <li>1 — 'Do Not Decrypt'</li> <li>2 — 'Block'</li> </ul>		• 1 — 'Do Not Decrypt'
		• 2 — 'Block'
		• 3 — 'Block With Reset'
• 4 — 'Decrypt (Known Key)'		• 4 — 'Decrypt (Known Key)'
		• 5 — 'Decrypt (Replace Key)'
		• 6 — 'Decrypt (Resign)'

Table B-8 Intrusion Event Record 6.x Fields (continued)

Field	Data Type	Description
SSL Flow Status	uint16	Status of the SSL Flow. These values describe the reason behind the action taken or the error message seen. Possible values include:
		• 0 — 'Unknown'
		• 1 — 'No Match'
		• 2 — 'Success'
		• 3 — 'Uncached Session'
		• 4 — 'Unknown Cipher Suite'
		• 5 — 'Unsupported Cipher Suite'
		• 6 — 'Unsupported SSL Version'
		• 7 — 'SSL Compression Used'
		8 — 'Session Undecryptable in Passive Mode'
		• 9 — 'Handshake Error'
		• 10 — 'Decryption Error'
		• 11 — 'Pending Server Name Category Lookup'
		• 12 — 'Pending Common Name Category Lookup'
		• 13 — 'Internal Error'
		• 14 — 'Network Parameters Unavailable'
		• 15 — 'Invalid Server Certificate Handle'
		• 16 — 'Server Certificate Fingerprint Unavailable'
		• 17 — 'Cannot Cache Subject DN'
		• 18 — 'Cannot Cache Issuer DN'
		• 19 — 'Unknown SSL Version'
		• 20 — 'External Certificate List Unavailable'
		• 21 — 'External Certificate Fingerprint Unavailable'
		• 22 — 'Internal Certificate List Invalid'
		• 23 — 'Internal Certificate List Unavailable'
		• 24 — 'Internal Certificate Unavailable'
		• 25 — 'Internal Certificate Fingerprint Unavailable'
		• 26 — 'Server Certificate Validation Unavailable'
		• 27 — 'Server Certificate Validation Failure'
		• 28 — 'Invalid Action'
Network Analysis Policy UUID	uint8[16]	The UUID of the Network Analysis Policy that created the intrusion event.
HTTP Response	uint32	Response code of the HTTP Request.

### **Intrusion Event Record 7.0**

The fields in the intrusion event record are shaded in the following graphic. The record type is 400 and the block type is 81 in the series 2 set of data blocks. It supersedes block type 60, and is superseded by block type 85. Inline Result Reason, Ingress and Egress Virtual Route Forwarding, and Snort Version fields have been added. The Blocked field has been renamed Inline Result.

You can request 7.0 intrusion events from eStreamer only by extended request, for which you request event type code 12 and version code 10in the Stream Request message (see Submitting Extended Requests, page 2-4 for information about submitting extended requests).

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			
	Header Ve	ersion (1)	Message	Type (4)			
		Message	Length				
	Netma	ap ID	Record T	ype (400)			
		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)			
	Block Type (81)						
		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						
		Classific	ation ID				
		Priori	ty ID				

Byte	0						1							2							3										
Bit	0 1 2 3 4 5 6 7					8	ç	$\frac{1}{0}$	1 1		1 1 2	1 1 4	1 5		1 7		1 1 8 9		1	2 2	$\begin{bmatrix} 2 & 2 \\ 2 & 3 \end{bmatrix}$		2 4	2 2 6		2 7	2 2	2	3 3 1		
		Source IP Address																													
		Source IP Address, continued																													
		Source IP Address, continued																													
											Sou	ıro	ce I	РΑ	dc	dres	s, c	cc	ntir	nuec	d 										
											]	D	esti	inat	ioı	n IP	A	do	lres	s											
														n IP																	
														n IP																	
										De	stir	ıa	atio	n IP	A	\dd1	ess	ς,	con	tinı	ue	ed									
			S	ourc	ce l	Po	ort o	r IO	CI	MP	Туј	ре	e						Des	tina	ıti	on	Por	t	or l	[CM	1P	C	ode		
	IP	Pr	ot	oco	ol II	D				Imp	act	t I	Flag	gs					Im	pac	t					Inli	in	e R	Resu	lt	
	In			Res		t						MPLS Label																			
	MPL	S	La	abel	l, c	OI	nt.		VLAN ID								Pad														
	I	Pac	d,	Coı	nt.												F	C	licy	UI	UI	ID									
											P	o	olic	y U	UI	D,	con	ıti	inue	d											
											P	o	olic	y U	UI	D,	con	ıti	inue	d											
											P	o	olic	y U	UI	D,	con	ıti	inue	d											
							F	oli	ic:	y Ul	JII	Э,	, co	ntin	ue	ed										Į	Us	ser	ID		
								U	Js	er II	Ο, σ	cc	onti	nue	d										W	/eb	A	pp ID	lica	tio	n
						1	Web	Aj	pŗ	olica	tio	n	ID	, co	nti	inue	ed								Cl	ient		App ID	olica	atio	on
								Cli	ie	nt A	pp	li	icat	ion	ID	)										Apj	p.	Pr	ot. l	D	
					A	Ąр	pplic	ati	OI	n Pr	oto	C	ol I	D, 0	COI	ntin	uec	d							A	cce	SS	S C	trl F	Rul	le
		Access Control Rule ID, continued  Acc. Ctrl Policy UUID								у																					
								1	A	cces	s C	Co	ontr	ol P	ol	icy	UU	J	D, 0	con	tiı	nue	d								
								1	A	cces	s C	Co	ontr	ol P	ol	icy	UU	J]	D, 0	con	tir	nue	d								

Byte	0	1	2	3					
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	9   1   1   1   1   1   1   1   1   1						
		Access Control Poli	cy UUID, continued						
	Access C	Int. Ingress UUID							
		Interface Ingress	UUID, continued						
		Interface Ingress	UUID, continued						
		Interface Ingress	UUID, continued						
	Interfa	ce Ingress UUID, con	tinued	Int. Egress UUID					
		Interface Egress	UUID, continued						
		Interface Egress	UUID, continued						
		Interface Egress	UUID, continued						
	Interfa	ace Egress UUID, cont	inued	Sec. Zone Ing. UUID					
		,							
		Security Zone Ingre	ss UUID, continued						
		Security Zone Ingre	ss UUID, continued						
	Security	Zone Ingress UUID, c	ontinued	Sec. Zone Egr. UUID					
		Security Zone Egre	ss UUID, continued						
		Security Zone Egre	ss UUID, continued						
		Security Zone Egre	ss UUID, continued						
	Security	Zone Egress UUID, co	ontinued	Cxn Timestamp					
	Conne	ction Timestamp, con	tinued	Connection Inst. ID					
	Connection Inst. ID	Connection	n Counter	Source Country					
	Source Country	Destinatio	Destination Country						
	IOC Number		Security Context						
		Security Cont	ext, continued						
		Security Cont	ext, 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 2 6 7 8 9 0 1 2 3	2 2 2 2 2 3 3 4 5 6 7 8 9 0 1							
		Security Conte	ext, continued								
	Sec. Context, cont.	SSL Certificate Fingerprint									
		SSL Certificate Fin	gerprint, continued								
		SSL Certificate Fin	gerprint, continued								
		SSL Certificate Fin	gerprint, continued								
		SSL Certificate Fin	gerprint, continued								
	SSL Cert. Fngpt, cont.	SSL Actu	al Action	SSL Flow Status							
	SSL Flow Stat., cont.	Network Analysis Policy UUID									
		Network Analysis Pol	icy UUID, continued								
		Network Analysis Pol	etwork Analysis Policy UUID, continued								
		Network Analysis Pol									
	Net A. P. UUID, cont.										
Iı	HTTP Resp,, cont.										
Ingress VRF	String Block Type (0)	String Block Length									
RF	String Block Length										
Egi		String Bloc	k Type (0)								
gress VRF		String Blo	ck Length								
RF		Egress VI	RF Name								
	Snort Version										

The following table describes each intrusion event record data field.

Table B-9 Intrusion Event Record 7.0 Fields

Field	Data Type	Description
Block Type	unint32	Initiates an Intrusion Event data block. This value is always 81.
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 3-33 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 Secure Firewall 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 ID	uint8	IANA-specified protocol number. For example:
		• 0 — IP
		• 1 — ICMP
		• 6 — TCP
		• 17 — UDP

Table B-9 Intrusion Event Record 7.0 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 Secure Firewall 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 Management Center. An x indicates the value can be 0 or 1:
		• gray (0, unknown): 00x00000
		• red (1, vulnerable): xxxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx (version 5.0+ only)
		• orange (2, potentially vulnerable): 00x0011x
		• yellow (3, currently not vulnerable): 00x0001x
		• blue (4, unknown target): 00x00001
Impact	uint8	Impact flag value of the event. Values are:
		• 1 — Red (vulnerable)
		• 2 — Orange (potentially vulnerable)
		• 3 — Yellow (currently not vulnerable)
		• 4 — Blue (unknown target)
		• 5 — Gray (unknown impact)

Table B-9 Intrusion Event Record 7.0 Fields (continued)

Field	Data Type	Description			
Inline Result	uint8	Value indicating the inline result.			
		• 0 — Pass			
		• 1 — Dropped			
		• 2 — Would be dropped (but not permitted by configuration)			
		3— Partially dropped			
Inline Result	uint8	Value indicating the inline result reason.			
Reason		• 1— Interface in Passive or Tap mode			
		• 2— Intrusion Policy in "Detection" inspection mode			
		• 3— Network Analysis Policy in "Detection" inspection mode			
		• 4— Connection timed out			
		• 5— Connection Closed (internal use)			
		• 6— Connection Closed (internal use)			
		• 7— Connection Closed (internal use)			
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.			
Interface Ingress UUID	uint8[16]	An interface ID number that acts as a unique identifier for the ingress interface.			
Interface Egress UUID	uint8[16]	An interface ID number that acts as a unique identifier for the egress interface.			
Security Zone Ingress UUID	uint8[16]	A zone ID number that acts as a unique identifier for the ingress security zone.			
Security Zone Egress 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.			

Table B-9 Intrusion Event Record 7.0 Fields (continued)

Field	Data Type	Description			
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.			
SSL Certificate Fingerprint	uint8[20]	SHA1 hash of the SSL Server certificate.			
SSL Actual Action	uint16	The action performed on the connection based on the SSL Rule. This may differ from the expected action, as the action as specified in the rule may be impossible. Possible values include:  • 0 — 'Unknown'			
		• 1 — 'Do Not Decrypt'			
		• 2 — 'Block'			
		• 3 — 'Block With Reset'			
		• 4 — 'Decrypt (Known Key)'			
		• 5 — 'Decrypt (Replace Key)'			
		• 6 — 'Decrypt (Resign)'			

Table B-9 Intrusion Event Record 7.0 Fields (continued)

Field	Data Type	Description
SSL Flow Status	uint16	Status of the SSL Flow. These values describe the reason behind the action taken or the error message seen. Possible values include:
		• 0 — 'Unknown'
		• 1 — 'No Match'
		• 2 — 'Success'
		• 3 — 'Uncached Session'
		• 4 — 'Unknown Cipher Suite'
		• 5 — 'Unsupported Cipher Suite'
		• 6 — 'Unsupported SSL Version'
		• 7 — 'SSL Compression Used'
		8 — 'Session Undecryptable in Passive Mode'
		• 9 — 'Handshake Error'
		• 10 — 'Decryption Error'
		• 11 — 'Pending Server Name Category Lookup'
		• 12 — 'Pending Common Name Category Lookup'
		• 13 — 'Internal Error'
		• 14 — 'Network Parameters Unavailable'
		• 15 — 'Invalid Server Certificate Handle'
		• 16 — 'Server Certificate Fingerprint Unavailable'
		• 17 — 'Cannot Cache Subject DN'
		• 18 — 'Cannot Cache Issuer DN'
		• 19 — 'Unknown SSL Version'
		• 20 — 'External Certificate List Unavailable'
		• 21 — 'External Certificate Fingerprint Unavailable'
		122 — 'Internal Certificate List Invalid'
		• 23 — 'Internal Certificate List Unavailable'
		• 24 — 'Internal Certificate Unavailable'
		• 25 — 'Internal Certificate Fingerprint Unavailable'
		26 — 'Server Certificate Validation Unavailable'
		27 — 'Server Certificate Validation Failure'
		28 — 'Invalid Action'
Network Analysis Policy UUID	uint8[16]	The UUID of the Network Analysis Policy that created the intrusion event.
HTTP Response	uint32	Response code of the HTTP Request.

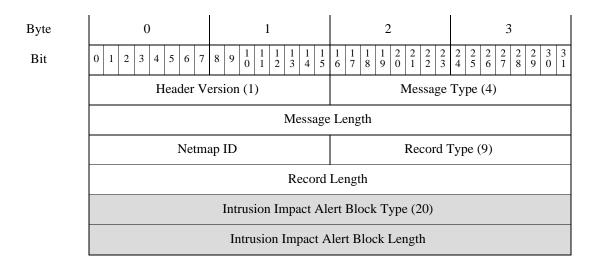
Table B-9	Intrusion	Event Record	7 O Field	s (continued)
า สมาช อ-ฮ	แแนนรเบน	Eveiil necoiu	7.0 Field	s (COIILIIIueu/

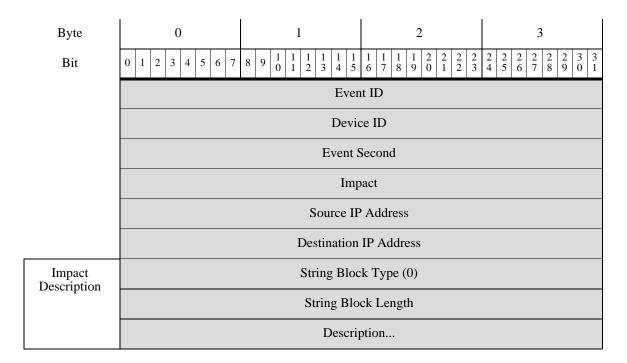
Field	Data Type	Description
String Block Type	uint32	Initiates a String data block containing the name of the ingress VRF. This value is always 0.
String Block Length	uint32	The number of bytes included in the name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Ingress VRF name field.
Ingress VRF Name	string	The virtual router through which traffic entered the network.
String Block Type	uint32	Initiates a String data block containing the name of the egress VRF. This value is always 0.
String Block Length	uint32	The number of bytes included in the name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Egress VRF name field.
Egress VRF Name	string	The name of the virtual router through which traffic exited the network.
Snort Version	uint8	Snort version number.

## **Intrusion Impact Alert Data**

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 4-62.)

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 2-12 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.





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

Table B-10 Impact Event Data Fields

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

Table B-10 Impact Event Data Fields (continued)

Field	Data Type	Description
Impact	bits[8]	Impact flag value of the event. The low-order eight bits indicate the impact level. Values are:
		• 0x01 (bit 0) — Source or destination host is in a network monitored by the system.
		• 0x02 (bit 1) — Source or destination host exists in the network map.
		• 0x04 (bit 2) — Source or destination host is running a server on the port in the event (if TCP or UDP) or uses the IP protocol.
		• 0x08 (bit 3) — There is a vulnerability mapped to the operating system of the source or destination host in the event.
		• 0x10 (bit 4) — There is a vulnerability mapped to the server detected in the event.
		• 0x20 (bit 5) — The event caused the managed device to drop the session (used only when the device is running in inline, switched, or routed deployment). Corresponds to blocked status in the Secure Firewall 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
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 4-71.

Table B-10 Impact Event Data Fields (continued)

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

#### **Intrusion Event Extra Data Record**

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

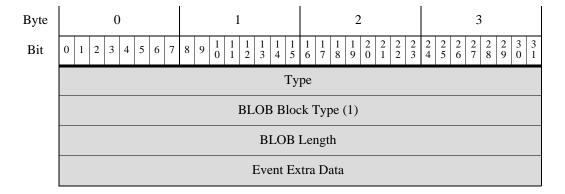
This record is deprecated in version 7.1. While it can still be requested no records will be generated.

The event extra data appears in an encapsulated Event Extra Data data block, which always has a data block type value of 4. (The Event Extra Data data block is a series 2 data block. For more information about series 2 data blocks, see Understanding Series 2 Data Blocks, page 3-53.)

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

If bit 27 is set in the Request Flags field of the request message, you receive the event extra data for each intrusion event. If you set bit 20, you also receive the event extra data metadata described in Intrusion Event Extra Data Metadata, page B-66. If you enable bit 23, eStreamer will include the extended event header. See Request Flags, page 2-13 for information on setting request flags.

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														
	Netmap ID Record Type (110)														
	Record Length														
	eStream	ner Server Timestamp (	in events, only if bit 23	3 is set)											
	Rese	rved for Future Use (in	events, only if bit 23 is	s set)											
		Event Extra Data D	ata Block Type (4)												
		Event Extra Data I	Data Block Length												
		Devic	ee ID												
		Even	t ID												
		Event S	Second												



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

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

Table B-11 Intrusion Event Extra Data Block Fields

Field	Data Type	Description
Event Extra Data Data Block Type	uint32	Initiates an Event Extra Data data block. This value is always 4. The block type is a series 2 block; for information see Understanding Series 2 Data Blocks, page 3-53.
Event Extra Data Data Block Length	uint32	Length of the data block. Includes the number of bytes of data plus the 8 bytes in the two data block header fields.
Device ID	uint32	The managed device identification number.
Event ID	uint32	The event identification number.
Event Second	uint32	UNIX timestamp of the event (seconds since 01/01/1970).
Туре	uint32	Identifier for the type of extra data; for example:  • 2 — XFF client (IPv6)  • 9 — HTTP URI
BLOB Block Type	uint32	Initiates a BLOB data block containing extra data. This value is always 1. The block type is a series 2 block.
Length	uint32	Total number of bytes in the BLOB data block.
Extra Data	variable	The content of the extra data. The data type is indicated in the Type field.

### **Intrusion Event Extra Data Metadata**

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

This record is deprecated in version 7.1. While it can still be requested no records will be generated.

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

If bit 20 is set in the Request Flags field of a request message, you receive the event extra data metadata. If you want to receive both intrusion events and event extra data metadata, you must set bit 2 as well. See Request Flags, page 2-13. If you enable bit 23, an extended event header is included in the record.

Byte	0	1	2	3
Bit	0 1 2 3 4 5 6 7	8 9 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	
	Netma	ap ID	Record T	ype (111)
		Record	Length	
	eStream	er 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)
	Ev	vent Extra Data Metada	ata Data Block Type (5	5)
		Data Bloc	k Length	
		Ту	ре	
		String Bloc	k Type (0)	
		String Blo	ck Length	
		Nan	ne	
		String Bloc	k Type (0)	
		String Blo	ck Length	
		Enco	ding	

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

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

Table B-12 Event Extra Data Metadata Data Block Fields

Field	Data Type	Description							
Event Extra Data Metadata Data Block Type	uint32	Initiates an Event Extra Data Metadata data block. This value is always 5. This block type is a series 2 block.							
Event Extra Data Metadata Data Block Length	uint32	Length of the data block. Includes the number of bytes of data plus the 8 bytes in the two data block header fields.							

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

Field	Data Type	Description
Туре	uint32	The type of extra data. Matches the Type field in the associated Event Extra Data record. This field is the unique key for this record.
String Block Type	uint32	Initiates a String data block for the client application version. This value is always 0. This block type is a series 2 block.
String Block Length	uint32	Number of bytes in the client application version String data block, including eight bytes for the string block type and length fields, plus the number of bytes in the version string.
Name	string	Name of the type of event extra data, for example, XFF client (IPv6), and HTTP URI.
String Block Type	uint32	Initiates a string data block for the client application URL. This value is always 0. This block type is a series 2 block.
String Block Length	uint32	Number of bytes in the client application URL String data block, including eight bytes for the string block type and length fields, plus the number of bytes in the URL string.
Encoding	string	Encoding used for the event extra data, for example, IPv4, IPv6, or string.

# **Legacy Malware Event Data Structures**

- Malware Event Data Block 5.1, page B-68
- Malware Event Data Block 5.1.1.x, page B-72
- Malware Event Data Block 5.2.x, page B-78
- Malware Event Data Block 5.3, page B-85
- Malware Event Data Block 5.3.1, page B-92
- Malware Event Data Block 5.4.x, page B-99
- Malware Event Data Block 6.x, page B-110

#### **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.

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

Byte		1										2									3												
Bit	0 1	2	3	4	5 6	7	7 8 9 1 1 1 1 1 1 1 1 1 1 1 1 1 1 7												1 8	1 9		2	2 2	2	2 3	2 4	2 5	2 6	7	28	2 2	3	3
									N	Mal	lw	are	e I	Ξve	ent	B	lo	ck	Т	ype	e (	(16)	)										
										M	al	wa	re	Ev	/ei	nt ]	Bl	oc]	k	Lei	ng	gth											
														Ag	en	t L	JU	ID	)														
											A	ge	nt	U	UI	D,	, C	on	tir	nue	d												
											A	ge	nt	U	UI	D,	C	on	tir	nue	d												
		Agent UUID, continued																															
		Cloud UUID																															
		Cloud UUID, continued																															
		Cloud UUID, continued																															
	Cloud UUID, continued																																
	Timestamp																																
	_		~ .										E	lve	nt	Ту	_			_													
					pe II				_									Ho	st	IP		Add							(0)				
Detection Name	Но		P A		ress,	,			D	ete	ct	or	IL	)							S	Strii	ng .	ВІ	oc	k '	ľyŗ	e	(0)				
			Strii	ng	Bloc	ck '	Ту	pe (	(0	), c	coı	nt.									i	Str	ng	В	loc	ck	Le	ng	gth				
			Stri	ng	Blo	ck	L	eng	th	, co	on	t.										D	ete	eti	on	N	am	ıe.					
User											,	Str	in	g E	Blo	ock	T	ур	e	(0)	)												
												St	riı	ng i	B1	oc]	k ]	Lei	ng	gth													
																ser																	
File Name											,			g E							)												
												St		ng i					_	gth													
														Fil																			
File Path														g E							)												
												St	riı	ng :					ng	gth													
														Fi	le	Pa	th	•••															

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 3 3 4 5 6 7 8 9 0 1		
File SHA Hash	String Block Type (0)					
Пазіі	String Block Length					
	File SHA 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 Block Type (0)					
SHA Hasii	String Block Length					
	Parent File SHA Hash					
Event Description	String Block Type (0)					
Sescription	String Block Length					
	Event Description					

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

Table B-13 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 AMP for Endpoints 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-13 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 o.	
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.	

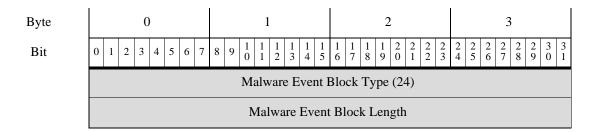
Table B-13 Malware Event Data Block Fields (continued)

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.

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



Byte	0	1	2	3
Bit	0 1 2 3 4 5 6 7	8 9 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 UUIE	), continued	
		Cloud UUIE	), 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 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	
		Use	r	
File Name		String Bloc	k Type (0)	
	String Block Length			
	File Name			
File Path		String Bloc	k 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     2     3     3       6     7     8     9     0     0     1     2     3     4     5     6     7     8     9     0	
File SHA	String Block Type (0)			
Hash	String Block Length			
		File SHA 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	k Type (0)	
SIIIIII		String Blo	ck Length	
		Parent File S	SHA Hash	
Event Description	String Block Type (0)			
	String Block Length			
	Event Description			
		Devid	ce ID	
	Connection	n Instance	Connection Counter	
		Connection Ev	ent Timestamp	
	Direction		Source IP Address	
		Source IP Add		
	Source IP Address, continued			
	Source IP Address, continued			
	Source IP, cont.		Destination IP Address	
	Destination IP Address, continued			
		Destination IP Ac		
		Destination IP Ac	udress, 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, cont		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)
	String	g Block Type (0), conti	nued	String Block Length
	Strin	g Block Length, contin	nued	URI
	Sourc	e Port	Destinat	ion Port

Table B-14 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 AMP for Endpoints 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-14 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 o.	

Table B-14 Malware Event Data Block for 5.1.1.x Fields (continued)

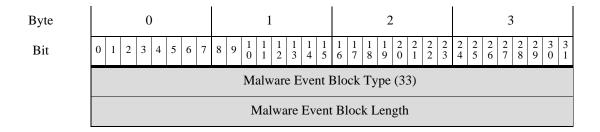
Field	Data Type	Description	
String Block Length	uint32	The number of bytes included in the Parent File Name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Parent File Name field.	
Parent File Name	string	The name of the file accessing the 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-14 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 Ever	nt Timestamp	
		Event T	ype ID	
Detection Name	Event Subtype ID	Detector ID	String Bloc	k Type (0)
	String Block 7	Гуре (0), cont.	String Blo	ck Length
	String Block Length, cont.  Detection Name			Name
User	String Block Type (0)			
		String Blo	ck Length	
	User			
File Name		String Bloc	k Type (0)	
	String Block Length			
	File Name			
File Path		String Bloc		
		String Blo		
	File Path			
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 1 5	1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 2 2 2 3 3 5 6 7 8 9 0 1	
		File	Туре	
		File Tir	mestamp	
Parent File Name		String Blo	ock Type (0)	
Trume		String Blo	ock Length	
		Parent Fi	ile Name	
Parent File SHA Hash		String Blo	ock Type (0)	
SILLITUSII		String Blo	ock Length	
		Parent File	SHA Hash	
Event Description		String Blo	ock Type (0)	
		String Blo	ock Length	
		Event Description		
	Device ID			
	Connection Instance Connection Counter			
	Connection Event Timestamp			
	Direction Source IP Address		Source IP Address	
		Source IP Add	dress, continued	
			dress, continued	
		Source IP Add	dress, continued	
	Source IP, cont.		Destination IP Address	
		Destination IP A	Address, continued	
	Destination IP Address, continued			
		Destination IP A	Address, continued	
	Destination IP, cont		Application ID	
	App. ID, cont.		User ID	
	User ID, cont.	Ac	ccess Control Policy UUID	

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
		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			ion Port
	Source Country Destination Country			n Country
	Web Application ID			
	Client Application ID			
	Action	Protocol		

Table B-15 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 AMP for Endpoints 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 o.

Table B-15 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 o.
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 o.

Table B-15 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	The number of bytes included in the Event Description St 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-15 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 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.		
<b>Destination Country</b>	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-15 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 Allow List
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				(	)					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	2	2 2	2 3	2 4	2 5	2 6	2 7	2 8	2	3 3 0 1
		Malware Event Block Type (35)																													
		Malware Event Block Length																													
		Agent UUID																													
												A	Age	nt	U	JID	), c	on	tinı	ied	i										
												A	Age	ent	UU	JID	), c	on	tinı	iec	i										
		Agent UUID, continued																													
		Cloud UUID																													
												C	Clo	ud	U	JID	), c	on	tinı	ied	i										

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 UUII	O, continued				
		Cloud UUII	), continued				
		Malware Even	nt Timestamp				
		Event T	Sype ID				
		Event Su	btype ID				
Detection Name	Detector ID		String Block Type (0)				
Tume	String Block Type (0), cont.		String Block Length				
	String Block Length, cont.		Detection Name				
User	String Block Type (0)						
	String Block Length						
		Use	er				
File Name		String Block Type (0)					
		String Blo	ck Length				
		File N	ame				
File Path		String Bloc	ek Type (0)				
		String Blo	ck Length				
		File P	ath				
File SHA Hash		String Bloc	ek Type (0)				
		String Blo	ck Length				
		File SHA Hash					
		File	Size				
		File 7	Гуре				
		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 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 3 4 5 6 7 8 9 0 1			
Parent File Name		String Block Type (0)					
rvanic		String Blo	ock Length				
		Parent Fil	le Name				
Parent File SHA Hash		String Bloo	ck Type (0)				
		String Blo	ock Length				
		Parent File	SHA Hash				
Event Description		String Bloo	ck Type (0)				
2 computer		String Blo	ock Length				
		Event Des	scription				
	Device ID						
	Connection Instance Connection Counter						
	Connection Event 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.	Ac	cess Control Policy U	UUID			

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 Block Type (0), continued  String Block Length						
	String Block Length, continued URI						
	Source	e Port	Destinat	ion Port			
	Source C	Country	Destination	n Country			
		Web Application ID					
		Client Application ID					
	Action	Protocol	Threat Score	IOC Number			
	IOC Number, cont.						

Table B-16 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 AMP for Endpoints 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-16 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 o.
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. The meaning of this field is transmitted in the metadata with this event. See AMP for Endpoints File Type Metadata, page 3-38 for more information.
File Timestamp	uint32	UNIX timestamp (seconds since 01/01/1970) of the creation of the detected or quarantined file.

Table B-16 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 o.		
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 SH 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.		

Table B-16 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.
<b>Destination Country</b>	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-16 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 Allow List
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 2 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 2 2 2 6 7 8 9 0 1 2 3 4 5	2 2 2 2 3 3 5 6 7 8 9 0 1									
		Cloud UUID											
		Cloud UUID	), continued										
		Cloud UUID	), continued										
		Cloud UUID, continued											
		Malware Ever	nt Timestamp										
		Event T	ype 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	т										
File Name		String Bloc	k Type (0)										
		String Bloo	ck Length										
		File Na	ame										
File Path		String Bloc	k Type (0)										
		String Bloo	ck Length										
		File P	ath										
File SHA Hash	String Block Type (0)												
	String Block Length												
		File SHA Hash											
		File S											
		File 7											
		File Tim	estamp										

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								
Parent File Name		String Bloo	ck Type (0)									
Name		String Blo	ock Length									
	Parent File Name											
Parent File SHA Hash	String Block Type (0)											
SINTINGS		String Blo	ock Length									
		Parent File S	SHA Hash									
Event Description		String Block Type (0)										
1		String Blo	ock Length									
		Event Des	scription									
		Devi	ce ID									
	Connectio	n Instance	Connection	on Counter								
		Connection Ev	ent Timestamp									
	Direction		Source IP Address									
		Source IP Add	ress, continued									
			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, Application ID cont											
	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 3 3 4 5 6 7 8 9 0 1								
	Access Control Policy 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	e Port	Destinat	tion Port								
	Source 0	Country	Destinatio	on Country								
		Web Appl	ication ID									
		Client App	lication ID									
	Action	Protocol	Threat Score	IOC Number								
	IOC Number, cont.		Security Context									
		Security Conte	ext, continued									
	Security Context, continued											
		Security Conte	ext, continued									
	Security Cont., cont.											

Table B-17 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 AMP for Endpoints agent reporting the malware event.
Cloud UUID	uint8[16]	The internal unique ID of the Cisco Advanced Malware Protection cloud from which the malware event originated.

Table B-17 Malware Event Data Block for 5.3.1 Fields (continued)

Field	Data Type	Description
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.
File SHA Hash	string	The rendered string of the SHA-256 hash value of the detected or quarantined file.

Table B-17 Malware Event Data Block for 5.3.1 Fields (continued)

Field	Data Type	Description
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. The meaning of this field is transmitted in the metadata with this event. See AMP for Endpoints File Type Metadata, page 3-38 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-17 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.
<b>Destination Country</b>	uint 16	Code for the country of the destination host.

Table B-17 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 Allow List
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.

## **Malware Event Data Block 5.4.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 47 in the series 2 group of blocks. It supersedes block 44 and is superseded by block . Fields for SSL and file archive support have been added.

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 6 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 3 3 4 5 6 7 8 9 0 1								
		Malware Event E	Block Type (47)									
		Malware Event	Block Length									
		Agent UUID										
		Agent UUID, continued										
		Agent UUID, continued										
		Agent UUID	, continued									
		Cloud I	UUID									
		Cloud UUID	, continued									
		Cloud UUID	, continued									
		Cloud UUID	, continued									
		Malware Even	t Timestamp									
		Event T	ype ID									
		Event Sub	otype ID									
Detection Name	Detector ID	2	String Block Type (0)									
rvanic	String Block Type (0), cont.											
	String Block Length, cont.		Detection Name									
User		String Block	k Type (0)									
		String Bloc	ck Length									
	User											
File Name		String Block	k Type (0)									
		String Bloc	ck Length									
		File Na	nme									

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 2 2 2 2 2 2 2 2 3 4 5 6 7 8 9	2 3 3 9 0 1							
File Path	String Block Type (0)										
		String Blo	ock Length								
	File Path										
File SHA Hash		String Blo	ck Type (0)								
114011		String Blo	ock Length								
	File SHA Hash										
		File Size									
		File	Туре								
		File Tir	mestamp								
Parent File Name		String Blo	ck Type (0)								
		String Blo	ock Length								
		Parent Fi	le Name								
Parent File SHA Hash		String Blo	ck Type (0)								
			ock Length								
			SHA Hash								
Event Description			ck Type (0)								
			ock Length								
			scription								
			ice ID								
	Connectio	on Instance	Connection Counter								
	Connection Event Timestamp										
	Direction Source IP Address										
	Source IP Address, continued  Source IP Address, continued										
			dress, continued								
	Source IP, cont.		Destination IP Address								

Byte	0	1				2								3						
Bit	0 1 2 3 4 5 6 7	8 9	$\begin{array}{c ccc} 1 & 1 & 1 \\ 0 & 1 & 2 \end{array}$	1 1 3 4	1 5	1 1 6 7		1 1 8 9		2 2	2 2 2		2 2 4	2 5	2 2	2	2 8	2 :		3
		D	estinat	ion IP	Ac	ddres	s,	con	tin	ue	d									
		D	estinat	ion IP	Αc	ddres	s,	con	tin	ue	d									
		Destination IP Address, continued																		
	Destination IP, cont					A	\p <sub>j</sub>	plic	ati	on	ID									
	App. ID, cont.							Use	er I	D										
	User ID, cont.			A	Acc	cess (	Со	ntro	ol I	Pol	licy	U	UII	)						
		Acce	ess Coi	ntrol P	olio	cy U	UI	D, 0	cor	ntir	nue	d								
		Acce	ess Coi	ntrol P	olio	cy U	UI	D, 0	cor	ntir	nue	d								
		Acce	ess Coi	ntrol P	olio	cy U	UI	D, 0	cor	ntir	nue	d								
URI	AC Pol UUID, cont.	D	Disposit	ion		Re	tro	). D	isp	os	itio	n	S	tr.	Bloc	k	Ty	pe (	(0)	
	String	g Block	к Туре	(0), co	nti	nued	l						String Block Length							
	Strin	g Bloc	k Leng	th, co	ntir	nued									U.	R]	I			
	Source	e Port								D	est	ina	atio	tion Port						
	Source (	Country	y			Destination Country														
			V	Veb A <sub>l</sub>	pl	icatio	on	ID												
			C	lient A	pp	licati	ior	ı ID	)											
	Action		Protoc	ol			Tł	rea	t S	со	re			I	OC 1	Nι	ımb	er		
	IOC Number, cont.					Se	eci	ırity	C	on	itex	t								
			Secu	rity Co	nte	ext, c	coi	ntinı	uec	d										
	Security Context, continued																			
	Security Context, continued																			
	Security Cont., cont. SSL Certificate Fingerpri							rint	rint											
		SSI	L Certi	ficate l	Fin	gerp	rin	ıt, co	ont	tin	ued									
		SSI	L Certi	ficate l	₹in	gerp	rin	ıt, co	ont	tin	ued									

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     2     2     2     2     2       2     3     4     5     6     7     8     9     0     1     2     3	2 2 2 2 2 3 3 4 5 6 7 8 9 0 1
	SSL Ce	ertificate Fingerprint, continued	
	SSL Ce	ertificate Fingerprint, continued	
	SSL Cert Fpt, cont.	SSL Actual Action	SSL Flow Status
Archive SHA	SSL Flow Stat., cont.	String Block Type (0)	
	Str. Blk Type, cont.	String Block Type (0)	
	Str. Length, cont.	Archive SHA	
Archive Name	String Block Type (0)		
	String Block Length		
		Archive Name	
	Archive Depth		

Table B-18 Malware Event Data Block for 5.4.x Fields

Field	Data Type	Description
Malware Event Block Type	uint32	Initiates a malware event data block. This value is always 47.
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 AMP for Endpoints agent reporting the malware event.
Cloud UUID	uint8[16]	The internal unique ID of the Cisco Advanced Malware Protection 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.

Table B-18 Malware Event Data Block for 5.4.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 o.
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. The meaning of this field is transmitted in the metadata with this event. See AMP for Endpoints File Type Metadata, page 3-38 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.

Table B-18 Malware Event Data Block for 5.4.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-18 Malware Event Data Block for 5.4.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.
		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-18 Malware Event Data Block for 5.4.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 Allow List
		• 6 — Cloud Lookup Timeout
		• 7 — Custom Detection
		8 — Custom Detection Block
		• 9 — Archive Block (Depth Exceeded)
		• 10 — Archive Block (Encrypted)
		• 11 — Archive Block (Failed to Inspect)
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.
SSL Certificate Fingerprint	uint8[20]	SHA1 hash of the SSL Server certificate.

Table B-18 Malware Event Data Block for 5.4.x Fields (continued)

Field	Data Type	Description
SSL Actual Action	uint16	The action performed on the connection based on the SSL Rule. This may differ from the expected action, as the action as specified in the rule may be impossible. Possible values include:
		• 0 — 'Unknown'
		• 1 — 'Do Not Decrypt'
		• 2 — 'Block'
		• 3 — 'Block With Reset'
		• 4 — 'Decrypt (Known Key)'
		• 5 — 'Decrypt (Replace Key)'
		• 6 — 'Decrypt (Resign)'

Table B-18 Malware Event Data Block for 5.4.x Fields (continued)

Field	Data Type	Description
SSL Flow Status	uint16	Status of the SSL Flow. These values describe the reason
		behind the action taken or the error message seen.
		Possible values include:
		Possible values include:  • 0 — 'Unknown'  • 1 — 'No Match'  • 2 — 'Success'  • 3 — 'Uncached Session'  • 4 — 'Unknown Cipher Suite'  • 5 — 'Unsupported Cipher Suite'  • 6 — 'Unsupported SSL Version'  • 7 — 'SSL Compression Used'  • 8 — 'Session Undecryptable in Passive Mode'  • 9 — 'Handshake Error'  • 10 — 'Decryption Error'  • 11 — 'Pending Server Name Category Lookup'  • 12 — 'Pending Common Name Category Lookup'  • 13 — 'Internal Error'  • 14 — 'Network Parameters Unavailable'  • 15 — 'Invalid Server Certificate Handle'  • 16 — 'Server Certificate Fingerprint Unavailable'  • 17 — 'Cannot Cache Subject DN'  • 18 — 'Cannot Cache Issuer DN'  • 19 — 'Unknown SSL Version'  • 20 — 'External Certificate List Unavailable'  • 21 — 'External Certificate Fingerprint Unavailable'  • 22 — 'Internal Certificate List Invalid'  • 23 — 'Internal Certificate List Unavailable'
		<ul> <li>25 — 'Internal Certificate Fingerprint Unavailable'</li> <li>26 — 'Server Certificate Validation Unavailable'</li> </ul>
		• 27 — 'Server Certificate Validation Failure'
		• 28 — 'Invalid Action'
String Block Type	uint32	Initiates a String data block containing the Archive SHA. This value is always 0.

Table B-18	Malware Event Data Block for 5.4.x Fields (continu	ied)

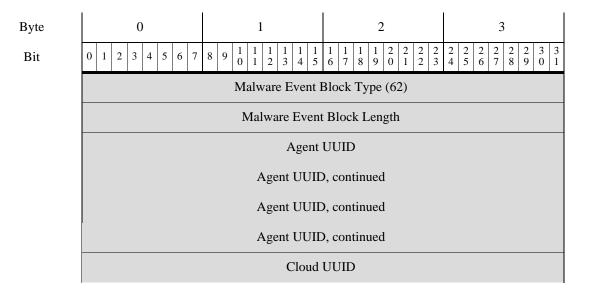
Field	Data Type	Description
String Block Length	uint32	The number of bytes included in the Archive SHA String data block, including eight bytes for the block type and header fields plus the number of bytes in the intrusion policy name.
Archive SHA	string	SHA1 hash of the parent archive in which the file is contained.
String Block Type	uint32	Initiates a String data block containing the Archive Name. This value is always 0.
String Block Length	uint32	The number of bytes included in the Archive Name String data block, including eight bytes for the block type and header fields plus the number of bytes in the intrusion policy name.
Archive Name	string	Name of the parent archive.
Archive Depth	uint8	Number of layers in which the file is nested. For example, if a text file is in a zip archive, this has a value of 1.

## **Malware Event Data Block 6.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 62 in the series 2 group of blocks. It supersedes block 47. A field for HTTP response has been added. It is superseded by block 80.

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 7 and an event code of 101.

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



Byte	0	1	2	3
Bit	0 1 2 3 4 5 6 7	8 9 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
		Cloud UUID	), continued	
	Cloud UUID, continued			
		Cloud UUIE	), continued	
		Malware Ever	nt Timestamp	
		Event T	ype ID	
		Event Su	btype ID	
Detection Name	Detector ID		String Block Type (0)	
1 (4111)	String Block Type (0), cont.		String Block Length	
	String Block Length, cont.		Detection Name	
User		String Bloc	k Type (0)	
		String Blo	ck Length	
		Use	т	
File Name	String Block Type (0)			
		String Blo	ck Length	
		File N	ame	
File Path		String Bloc	k Type (0)	
		String Blo	ck Length	
		File P	ath	
File SHA Hash		String Bloc	k Type (0)	
		String Blo	ck Length	
	File SHA Hash			
	File Size			
		File 7	Гуре	
		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 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 Blo	ck Length	
		Parent Fil	e Name	
Parent File SHA Hash		String Bloo	ck Type (0)	
SHA Hasii		String Blo	ck Length	
		Parent File S	SHA Hash	
Event Description		String Bloo	ck Type (0)	
Description		String Blo	ck Length	
		Event Des	scription	
	Device ID			
	Connection Instance Connection Counter		on Counter	
	Connection Event 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.	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	e Port	Destinat	ion Port
	Source (	Country	Destinatio	n Country
		Web Appl	ication ID	
		Client App	lication ID	
	Action	Protocol	Threat Score	IOC Number
	IOC Number, cont.		Security Context	
		Security Conte	ext, continued	
		Security Conte	ext, continued	
		Security Conte	ext, continued	
	Security Cont., cont.	SS	L Certificate Fingerpri	int
		SSL Certificate Fin	gerprint, continued	
		SSL Certificate Fin	gerprint, continued	
		SSL Certificate Fin	gerprint, continued	
		SSL Certificate Fin	gerprint, continued	
	SSL Cert Fpt, cont.	SSL Actu	al Action	SSL Flow Status
Archive SHA	SSL Flow Stat., cont.		String Block Type (0)	
	Str. Blk Type, cont.		String Block Type (0)	
	Str. Length, cont.		Archive SHA	

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     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
Archive Name		String Bloc	k Type (0)	
		String Blo	ck Length	
		Archive	Name	
	Archive Depth		HTTP Response	
	HTTP Resp., cont.			

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

Table B-19 Malware Event Data Block for 6.x Fields

Field	Data Type	Description
Malware Event Block Type	uint32	Initiates a malware event data block. This value is always 62.
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 AMP for Endpoints agent reporting the malware event.
Cloud UUID	uint8[16]	The internal unique ID of the AMP 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.

Table B-19 Malware Event Data Block for 6.x Fields (continued)

Field	Data Type	Description
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. The meaning of this field is transmitted in the metadata with this event. See AMP for Endpoints File Type Metadata, page 3-38 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 o.

Table B-19 Malware Event Data Block for 6.x Fields (continued)

Field	Data Type	Description
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.
Access Control Policy UUID	uint8[16]	Identification number that acts as a unique identifier for the access control policy that triggered the event.

Table B-19 Malware Event Data Block for 6.x 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 AMP cloud for a disposition, or the AMP 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-19 Malware Event Data Block for 6.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 Allow List
		• 6 — Cloud Lookup Timeout
		• 7 — Custom Detection
		8 — Custom Detection Block
		• 9 — Archive Block (Depth Exceeded)
		• 10 — Archive Block (Encrypted)
		• 11 — Archive Block (Failed to Inspect)
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.
SSL Certificate Fingerprint	uint8[20]	SHA1 hash of the SSL Server certificate.

Table B-19 Malware Event Data Block for 6.x Fields (continued)

Field	Data Type	Description
SSL Actual Action	uint16	The action performed on the connection based on the SSL Rule. This may differ from the expected action, as the action as specified in the rule may be impossible. Possible values include:
		• 0 — 'Unknown'
		• 1 — 'Do Not Decrypt'
		• 2 — 'Block'
		• 3 — 'Block With Reset'
		• 4 — 'Decrypt (Known Key)'
		• 5 — 'Decrypt (Replace Key)'
		• 6 — 'Decrypt (Resign)'

Table B-19 Malware Event Data Block for 6.x Fields (continued)

Field	Data Type	Description
SSL Flow Status	uint16	Status of the SSL Flow. These values describe the reason behind the action taken or the error message seen. Possible values include:
		• 0 — 'Unknown'
		• 1 — 'No Match'
		• 2 — 'Success'
		• 3 — 'Uncached Session'
		• 4 — 'Unknown Cipher Suite'
		• 5 — 'Unsupported Cipher Suite'
		• 6 — 'Unsupported SSL Version'
		• 7 — 'SSL Compression Used'
		8 — 'Session Undecryptable in Passive Mode'
		• 9 — 'Handshake Error'
		• 10 — 'Decryption Error'
		• 11 — 'Pending Server Name Category Lookup'
		• 12 — 'Pending Common Name Category Lookup'
		• 13 — 'Internal Error'
		• 14 — 'Network Parameters Unavailable'
		• 15 — 'Invalid Server Certificate Handle'
		• 16 — 'Server Certificate Fingerprint Unavailable'
		• 17 — 'Cannot Cache Subject DN'
		• 18 — 'Cannot Cache Issuer DN'
		• 19 — 'Unknown SSL Version'
		• 20 — 'External Certificate List Unavailable'
		• 21 — 'External Certificate Fingerprint Unavailable'
		• 22 — 'Internal Certificate List Invalid'
		• 23 — 'Internal Certificate List Unavailable'
		• 24 — 'Internal Certificate Unavailable'
		• 25 — 'Internal Certificate Fingerprint Unavailable'
		• 26 — 'Server Certificate Validation Unavailable'
		• 27 — 'Server Certificate Validation Failure'
		• 28 — 'Invalid Action'
String Block Type	uint32	Initiates a String data block containing the Archive SHA. This value is always 0.

Field	Data Type	Description
String Block Length	uint32	The number of bytes included in the Archive SHA String data block, including eight bytes for the block type and header fields plus the number of bytes in the intrusion policy name.
Archive SHA	string	SHA1 hash of the parent archive in which the file is contained.
String Block Type	uint32	Initiates a String data block containing the Archive Name. This value is always 0.
String Block Length	uint32	The number of bytes included in the Archive Name String data block, including eight bytes for the block type and header fields plus the number of bytes in the intrusion policy name.
Archive Name	string	Name of the parent archive.
Archive Depth	uint8	Number of layers in which the file is nested. For example, if a text file is in a zip archive, this has a value of 1.
HTTP Response	uint32	Response code of the HTTP Request.

Table B-19 Malware Event Data Block for 6.x Fields (continued)

# **Legacy Discovery Data Structures**

- Legacy Discovery Event Header, page B-121
- Legacy Server Data Blocks, page B-123
- Legacy Client Application Data Blocks, page B-124
- Legacy Scan Result Data Blocks, page B-125
- Legacy Host Profile Data Blocks, page B-150
- Legacy OS Fingerprint Data Blocks, page B-157

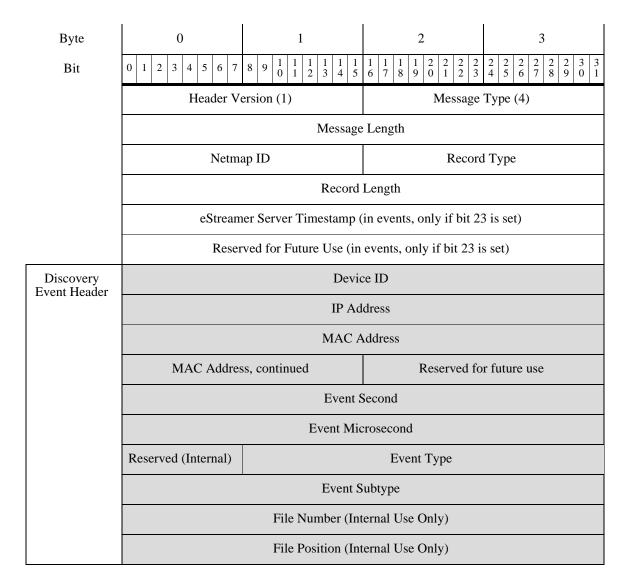
# **Legacy Discovery Event Header**

### **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 4-44.

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.



The following table describes the discovery event header.

Table B-20 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 3-33 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.

**Field Data Types Description** Event uint32 Microsecond (one millionth of a second) increment that the system Microsecond generated the event. Reserved byte Internal data from Cisco and can be disregarded. (Internal) 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 4-44 for a list of available event types. Event Subtype uint32 Event subtype. See Host Discovery Structures by Event Type, page 4-44 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.

Table B-20 Discovery Event Header Fields (continued)

# **Legacy Server Data Blocks**

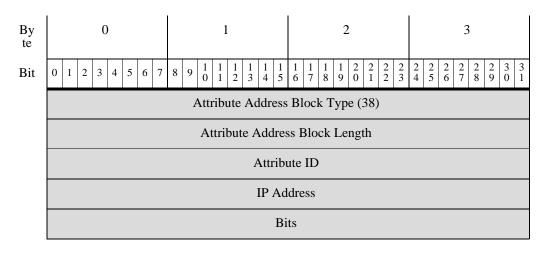
For more information, see the following sections:

• Attribute Address Data Block for 5.0 - 5.1.1.x, page B-123

#### 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:



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

Table B-21	Attribute	Address D	ata Block F	ields

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-124

### **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:

Byte	0	0 1		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 Client Application Block Type (59)				
	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-22 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.
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 4-59User Server Data Block Fields, page 4-103 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-126
- User Product Data Block for 5.0.x, page B-128
- User Information Data Block for 5.x, page B-148

#### 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 2	1 1 1 3 4 5	1 1 1 1 2 2 2 2 2 2 6 7 8 9 0 1 2 3 4	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1	
	Scan R	esult Blo	lock Type (102)		
	Scan	Result I	Block Length		
		Use	er ID		
		Scan	Туре		
		IP Ad	ddress		
	Port		Protoc	col	
	Flag		List Block T	Sype (11)	Scan Vulnerability
	List Block Type (11)		List Block	Length	List
Vulnerability List	List Block Length		Scan Vulnerability Block Type (109)		
	Scan Vulnerability Block Type (1	109)	Scan Vulnerability	Block Length	
	Scan Vulnerability Block Leng	th	Vulnerability	y Data	
	List Block Type (11)			Generic Scan Results List	
	List Block Length				11050115 2150
Scan Results List	Generic Scan Results Block Type (108)				
	Generic Scan Results Block Length				
	Generic Scan Results				
User Product List	Generic List Block Type (31)				
2 10 000 2250	Generic List Block Length				
	User l	Product	Data Blocks*		

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

Table B-23 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.	
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.	

Table B-23 Scan Result Data Block Fields (continued)

Field	Data Type	Description
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 4-171 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 Connection Statistics Data Block 6.0.x, page B-224 and User Server and Operating System Messages, page 4-57. 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 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 Block Type (65   118)					
	User Product Block Length					
	Source ID					
	Source Type					
IP Address Ranges	Generic List Block Type (31)					
Ranges	Generic List Block Length					
		IP Range Specificat	tion 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 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	
	Port Protocol			col	
		Drop Use	r Product		
Custom Vendor String	String Block Type (0)				
vendor string		String Blo	ck Length		
		Custom Ven	dor String		
Custom Product String		String Bloc	k Type (0)		
1 Todact String		String Blo	ck Length		
		Custom Prod	luct String		
Custom Version String		String Bloc	k Type (0)		
version string	String Block Length				
	Custom Version String				
	Software ID				
	Server ID				
	Vendor ID				
	Product ID				
Major Version String	String Block Type (0)				
		String Blo	ck Length		
	Major Version String				
Minor Version String	String Block Type (0)				
		String Block Length			
	Minor Version String				
Revision String Block Type (0)					
		String Blo	ck Length		
		Revision	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 1 1 1 1 1 2 2 2 2 2 2					
To Major String	String Block Type (0)					
Sumg	String Block Length					
		To Major <b>'</b>	Version String			
To Minor String		String B	lock Type (0)			
bumg		String F	Block Length			
		To Minor \	Version String			
To Revision String		String B	lock Type (0)			
Sumg		String F	Block Length			
		To Revi	sion String			
Build String		String B	lock Type (0)			
		String F	Block Length			
	Build String					
Patch String	String Block Type (0)					
		String F	Block Length			
		Patc	h String			
Extension String	String Block Type (0)					
		String F	Block Length			
		Extens	ion String			
OS UUID		Operating	System UUID			
	Operating System UUID cont.					
	Operating System UUID cont.					
	Operating System UUID cont.					
List of Fixes		Generic List	Block Type (31)			
		Generic Li	st Block Length			
		Fix List	Data Blocks*			

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

Table B-24 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 4-95 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	uint32	Indicates whether the user OS definition was deleted from the host:		
Product		• 0 — No		
		• 1 — Yes		
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.		

Table B-24 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 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.		
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.		

Table B-24 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 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.	
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.	

Field	Data Type	Description		
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 4-102 for a description of this data block.		

Table B-24 User Product Data Block Fields for 4.10.x, 5.0-5.0.x (continued)

## **Legacy User Login Data Blocks**

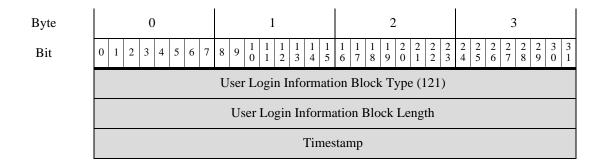
See the following sections for more information:

- User Login Information Data Block for 5.0 5.0.2, page B-134
- User Login Information Data Block 5.1-5.4.x, page B-136
- User Login Information Data Block 6.0.x, page B-138
- User Login Information Data Block 6.1.x, page B-141
- User Information Data Block for 5.x, page B-148

### **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 4-62.

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



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		
	IP Address					
User Name		String Bloc	k Type (0)			
Tunie	String Block Length					
	User Name					
	User ID					
	Application ID					
Email	String Block Type (0)					
	String Block Length					
		Ema	il			

Table B-25 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 o.	
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.	
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.	

Table B-25 User Login Information Data Block Fields 5.0 - 5.0.2 (continued)

Field	Data Type	Description
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.

#### **User Login Information Data Block 5.1-5.4.x**

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 Account Update Message Data Block, page 4-179.

The User Login Information data block has a block type of 73 for version 4.7 - 4.10.x, a block type of 121 in the series 1 group of blocks for version 5.0 - 5.0.2, and a block type of 127 in the series 1 group of blocks for version 5.1-5.4.x.

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				
	User Login Information Block Type (127)							
	User Login Information Block Length							
	Timestamp							
		IPv4 A	ddress					
User Name		String Block Type (0)						
Tvaine	String Block Length							
	User Name							
	User ID							
	Application ID							
Email	String Block Type (0)							
	String Block Length							
	Email							
	IPv6 Address							
	IPv6 Address, continued							
		IPv6 Address	s, 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     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
	IPv6 Address, continued			
Reported By	Login Type	n Type String Block Type (0)		
	String Block Type (0), cont.			
	String Block Length	Reported By		

Table B-26 User Login Information Data Block Fields

Field	Data Type	Description	
User Login Information Block Type	uint32	Initiates a User Login Information data block. This value is 127 for version 5.1+.	
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.	
IPv4 Address	uint32	This field is reserved but no longer populated. The IPv4 address is stored in the IPv6 Address field. See IP Addresses, page 1-4 for more information.	
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.	
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.	
IPv6 Address	uint8[16]	IPv6 address from the host where the user was detected logging in, in IP address octets.	

Table B-26 User Login Information Data Block Fields (continued)

Field	Data Type	Description
Login Type	uint8	The type of user login detected.
String Block Type	uint32	Initiates a String data block containing the Reported By value. This value is always 0.
String Block Length	uint32	Number of bytes in the Reported By String data block, including eight bytes for the block type and length fields, plus the number of bytes in the Reported By field.
Reported By	string	The name of the Active Directory server reporting a login.

#### **User Login Information Data Block 6.0.x**

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 Account Update Message Data Block, page 4-179.

he User Login Information data block has a block type of 159 for version 6.0.x. It has new ISE integration endpoint profile, Security Intelligence fields.

The User Login Information data block has a block type of 73 for version 4.7 - 4.10.x, a block type of 121 in the series 1 group of blocks for version 5.0 - 5.0.2, and a block type of 127 in the series 1 group of blocks for version 5.1+. See User Login Information Data Block 5.1-5.4.x, page B-136 for more information.

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
	User Login Information Block Type (159)			
	User Login Information Block Length			
		Times	stamp	
	IPv4 Address			
User Name	String Block Type (0)			
Tunic	String Block Length			
	User Name			
Domain	String Block Type (0)			
	String Block Length			
	Domain			
	User 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 2 6 7 8 9 0 1 2 3	2 2 2 2 2 3 3 4 5 6 7 8 9 0 1
		Realm ID		
		Endpoint Profile ID		
	Security Group ID			
		Prote	ocol	
Email		String Bloc	k Type (0)	
		String Blo	ck Length	
		Email		
	IPv6 Address			
		IPv6 Address, continued		
		IPv6 Addres	s, continued	
		IPv6 Addres	s, continued	
	Location IPv6 Address			
	Location IPv6 Address, continued			
	Location IPv6 Address, continued			
_	Location IPv6 Address, continued			
Reported By	Login Type	Auth. Type	String Bloo	ck Type (0)
	String Block 7	Type (0), cont.	String Blo	ock Length
	String Block Length, cont. Reported By			ed By

Table B-27 User Login Information Data Block Fields

Field	Data Type	Description
User Login Information Block Type	uint32	Initiates a User Login Information data block. This value is 159 for version 6.0.x.
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.

Table B-27 User Login Information Data Block Fields (continued)

Field	Data Type	Description	
IPv4 Address	uint32	This field is reserved but no longer populated. The IPv4 address is stored in the IPv6 Address field. See IP Addresses, page 1-4 for more information.	
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.	
Username	string	The user name for the user.	
String Block Type	uint32	Initiates a String data block containing the domain. 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 domain.	
Domain	string	Domain in which the user logged in.	
User ID	uint32	Identification number of the user.	
Realm ID	uint32	Integer ID which corresponds to an identity realm.	
Endpoint Profile ID	uint32	ID number of the type of device used by the connection endpoint. This is unique for each DC and resolved in metadata.	
Security Group ID	uint32	ID number of the network traffic group.	
Protocol	uint32	Protocol used to detect or report the user. Possible values are:  • 165 - FTP  • 426 - SIP  • 547 - AOL Instant Messenger  • 683 - IMAP  • 710 - LDAP  • 767 - NTP  • 773 - Oracle Database  • 788 - POP3  • 1755 - MDNS	
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.	
IPv6 Address	uint8[16]	IPv6 address from the host where the user was detected logging in, in IP address octets.	
Location IPv6 Address	uint8[16]	Most recent IP address on which the user logged in. Can be either an IPv4 or IPv6 address.	

Table B-27 User Login Information Data Block Fields (continued)

Field	Data Type	Description	
Login Type	uint8	The type of user login detected.	
Authentication Type	uint8	Type of authentication used by the user. Values may be:  o - no authorization required  1 - passive authentication, AD agent, or ISE session  2 - captive portal successful authentication  3 - captive portal guest authentication  4 - captive portal failed authentication	
String Block Type	uint32	Initiates a String data block containing the Reported By value. This value is always 0.	
String Block Length	uint32	Number of bytes in the Reported By String data block, including eight bytes for the block type and length fields, plus the number of bytes in the Reported By field.	
Reported By	string	The name of the Active Directory server reporting a login.	

### **User Login Information Data Block 6.1.x**

The User Login Information data block has a block type of 165 in the series 1 group of blocks for version 6.1+. It has new port and tunneling fields. It supersedes block type 159. See User Login Information Data Block 6.0.x, page B-138 for more information. It is superseded by block type 167.

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
		User Login Information	on Block Type (165)	
		User Login Information Block Length		
		Times	tamp	
	IPv4 Address			
User Name		String Block	k Type (0)	
Tunic	String Block Length			
	User Name			
Domain	String Block Type (0)			
	String Block Length			
		Doma	nin	

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
		Use	r ID	
		Realı	n ID	
		Endpoint 1	Profile ID	
		Security (	Group ID	
		Prot	ocol	
	Po	ort	Rang	e Start
	Start	Port	End	Port
Email	String Block Type (0)			
	String Block Length			
		Email		
		IPv6 A	ddress	
		IPv6 Addres	s, continued	
		IPv6 Addres	s, continued	
	IPv6 Address, continued			
	Location IPv6 Address			
	Location IPv6 Address, continued			
	Location IPv6 Address, continued			
	Location IPv6 Address, continued			
Reported By	Login Type	Auth. Type		ck Type (0)
	String Block Type (0), cont. String Block Length			-
	String Block	Length, cont.	Report	ed By

Table B-28 User Login Information Data Block Fields

Field	Data Type	Description	
User Login Information Block Type	uint32	Initiates a User Login Information data block. This value is 165 for version 6.1+.	
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.	
IPv4 Address	uint32	This field is reserved but no longer populated. The IPv4 address is stored in the IPv6 Address field. See IP Addresses, page 1-4 for more information.	
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.	
Username	string	The user name for the user.	
String Block Type	uint32	Initiates a String data block containing the domain. 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 domain.	
Domain	string	Domain in which the user logged in.	
User ID	uint32	Identification number of the user.	
Realm ID	uint32	Integer ID which corresponds to an identity realm.	
Endpoint Profile ID	uint32	ID number of the type of device used by the connection endpoint. This is unique for each DC and resolved in metadata.	
Security Group ID	uint32	ID number of the network traffic group.	
Protocol	uint32	Protocol used to detect or report the user. Possible values are:  • 165 - FTP  • 426 - SIP  • 547 - AOL Instant Messenger  • 683 - IMAP  • 710 - LDAP  • 767 - NTP  • 773 - Oracle Database  • 788 - POP3  • 1755 - MDNS	
Port	uint16	The port number on which the user was detected.	
	Jiii O	The post number on which the user was detected.	

Table B-28 User Login Information Data Block Fields (continued)

Field	Data Type	Description		
Range Start	uint16	The start port in the port range used by the TS Agent.		
Start Port	uint16	The start port in the range the TS Agent assigned to the individual user.		
End Port	uint16	The end port in the range the TS Agent assigned to the individual user.		
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.		
IPv6 Address	uint8[16]	IPv6 address from the host where the user was detected logging in, in IP address octets.		
Location IPv6 Address	uint8[16]	Most recent IP address on which the user logged in. Can be either an IPv4 or IPv6 address.		
Login Type	uint8	The type of user login detected.		
Authentication Type	uint8	Type of authentication used by the user. Values may be:		
		• 0 - no authorization required		
		• 1 - passive authentication, AD agent, or ISE session		
		• 2 - captive portal successful authentication		
		• 3 - captive portal guest authentication		
		• 4 - captive portal failed authentication		
String Block Type	uint32	Initiates a String data block containing the Reported By value. This value is always 0.		
String Block Length	uint32	Number of bytes in the Reported By String data block, including eight bytes for the block type and length fields, plus the number of bytes in the Reported By field.		
Reported By	string	The name of the Active Directory server reporting a login.		

# **User Login Information Data Block 6.1.x**

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 4-62.

The User Login Information data block has a block type of 165 in the series 1 group of blocks for version 6.1x. It has new port and tunneling fields. It supersedes block type 159. It is superseded by block type 167. See User Login Information Data Block 6.0.x, page B-138 for more information.

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 2 2 2 2 2 2 2 2					
	User Login Information Block Type (165)					
	User Login Information Block Length					
	Timestamp					
	IPv4 Address					
User Name	S	ring Block	Type (0)			
T varie	5	string Block	Length			
		User Naı	ne			
Domain	S	ring Block	Type (0)			
	S	string Block	Length			
		Domaii	n			
	User ID					
	Realm ID					
	Endpoint Profile ID					
	Security Group ID					
		Protoc	ol			
	Port		Range Start	Range Start		
	Start Port		End Port			
Email	S	ring Block	Type (0)			
	5	String Block	Length			
	Email					
	IPv6 Address					
	IPv6 Address, continued					
	IPv6 Address, continued					
	IPv6 Address, continued					
	Lo	ocation IPv6	5 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     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	
		Location IPv6 Ac	ldress, continued		
		Location IPv6 Ad	ldress, continued		
	Location IPv6 Address, continued				
Reported By	Login Type	Auth. Type	String Block Type (0)		
	String Block Type (0), cont. String Block Length				
	String Block Length, cont. Reported By				
Domain	String Block Type (0)				
	String Block Length				
	Description				

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

Table B-29 User Login Information Data Block Fields

Field	Data Type	Description	
User Login Information Block Type	uint32	Initiates a User Login Information data block. This value is 165 for version 6.2+.	
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.	
IPv4 Address	uint32	This field is reserved but no longer populated. The IPv4 address is stored in the IPv6 Address field. See IP Addresses, page 1-4 for more information.	
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.	
Username	string	The user name for the user.	
String Block Type	uint32	Initiates a String data block containing the domain. 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 domain.	

Table B-29 User Login Information Data Block Fields (continued)

Field	Data Type	Description	
Domain	string	Domain in which the user logged in.	
User ID	uint32	Identification number of the user.	
Realm ID	uint32	Integer ID which corresponds to an identity realm.	
Endpoint Profile ID	uint32	ID number of the type of device used by the connection endpoint. This is unique for each DC and resolved in metadata.	
Security Group ID	uint32	ID number of the network traffic group.	
Protocol	uint32	Protocol used to detect or report the user. Possible values are:  • 165 - FTP  • 426 - SIP  • 547 - AOL Instant Messenger  • 683 - IMAP  • 710 - LDAP  • 767 - NTP  • 773 - Oracle Database  • 788 - POP3	
		• 1755 - MDNS	
Port	uint16	The port number on which the user was detected.	
Range Start	uint16	The start port in the port range used by the TS Agent.	
Start Port	uint16	The start port in the range the TS Agent assigned to the individual user.	
End Port	uint16	The end port in the range the TS Agent assigned to the individual user.	
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.	
IPv6 Address	uint8[16]	IPv6 address from the host where the user was detected logging in, in IP address octets.	
Location IPv6 Address	uint8[16]	Most recent IP address on which the user logged in. Can be either an IPv4 or IPv6 address.	
Login Type	uint8	The type of user login detected.	
Authentication Type	uint8	Type of authentication used by the user. Values may be:	
		• 0 - no authorization required	
		• 1 - passive authentication, AD agent, or ISE session	
		• 2 - captive portal successful authentication	
		• 3 - captive portal guest authentication	
		• 4 - captive portal failed authentication	

Table B-29 User Login Information Data Block Fields (continued)

Field	Data Type	Description
String Block Type	uint32	Initiates a String data block containing the Reported By value. This value is always 0.
String Block Length	uint32	Number of bytes in the Reported By String data block, including eight bytes for the block type and length fields, plus the number of bytes in the Reported By field.
Reported By	string	The name of the Active Directory server reporting a login.

#### **User Information Data Block for 5.x**

The User Information data block is used in User Modification messages and conveys information for a user detected, removed, or dropped. For more information, see User Modification Messages, page 4-61

The User Information data block has a block type of 75 in the series 1 group of blocks for version 4.7 - 4.10.x and a block type of 120 in the series 1 group of blocks for 5.x. The structures are the same for block types 75 and 120.

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

Byte Bit	0     1     2     3       0     1     2     3       0     1     2     3       0     1     2     3       0     1     2     3       0     1     2     3       0     1     3       0     1     3       0     1     3       0     1     3       0     1     3       0     1     3       0     1     3       0     1     3       0     1     3       0     1     3       0     1     3       0     1     3       0     1     3       0     0     1       0     0     0       0     0     0       0     0     0       0     0     0       0     0     0       0     0     0       0     0       0     0       0     0       0     0       0     0       0     0       0     0       0     0       0     0			
Dit	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 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 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 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 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 7 8 9 0 1 2 3 4 5 6 7 8 8 9 1 2 3 4 5 6 7 8 8 9 1 2 3 4 5 7 8 8 9 1 2 3 4 5 7 8 8 9 1 2 3 4 5 7 8 8 9 1 2 3 4 5 7 8 8 9 1 2 3 4 5 7 8 8 9 1 2 3 4 5 7 8 8 9 1 2 3 4 5 7 8 8 9 1 2 3 4 5 7 8 8 9 1 2 3 4 5 7 8 8 9 1 2 3 4 5 7 8 8 9 1 2 3 4 5 7 8 8 9 1 2 3 4 5 7 8 7 8 7 8 7 8 7 8 7 8 7 8 7 8 7 8 7			
	User Information Block Length			
	User ID			
User Name	String Block Type (0)			
Tvarie	String Block Length			
	User Name			
	Protocol			
First Name	String Block Type (0)			
	String Block Length			
	First Name			
Last Name	String Block Type (0)			
	String Block Length			
	Last Name			

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		
Email	String Block Type (0)		
	String Block Length		
	Email		
Department	String Block Type (0)		
	String Block Length		
	Department		
Phone	String Block Type (0)		
	String Block Length		
	Phone		

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

Table B-30 User Information Data Block Fields

Field	Data Type	Description	
User Information Block Type	uint32	Initiates a User Information data block. This value is 75 for version 4.7 - 4.10.x and a value of 120 for 5.0+.	
User Information Block Length	uint32	Total number of bytes in the User Information data block, including eight bytes for the user information block type and length fields plus the number of bytes in the user information data that follows.	
User ID	uint32	Identification number of the user.	
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.	
Username	string	The username for the user.	
Protocol	uint32	The protocol for the packet containing the user information.	
String Block Type	uint32	Initiates a String data block containing the first name of the user. This value is always o.	
String Block Length	uint32	Number of bytes in the first name String data block, including eight bytes for the block type and length fields plus the number of bytes in the first name.	
First Name	string	The first name for the user.	
String Block Type	uint32	Initiates a String data block containing the last name for the user. This value is always 0.	

Table B-30 User Information Data Block Fields (continued)

Field	Data Type	Description	
String Block Length	uint32	Number of bytes in the user last name String data block, including eight bytes for the block type and length fields, plus the number of bytes in the last name.	
Last Name	string	The last name for the user.	
String Block Type	uint32	Initiates a String data block containing the email address for the user. This value is always o.	
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.	
String Block Type	uint32	Initiates a String data block containing the department for the user. This value is always 0.	
String Block Length	uint32	Number of bytes in the department String data block, including eight bytes for the block type and length fields, plus the number of bytes in the department.	
Department	string	The department for the user.	
String Block Type	uint32	Initiates a String data block containing the phone number for the user. This value is always o.	
String Block Length	uint32	Number of bytes in the phone number String data block, including eight bytes for the block type and length fields, plus the number of bytes in the phone number.	
Phone	string	The phone number 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-150

#### **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 1 5			
	Host Profile E	Block Type (91)		
	Host Profile	Block Length		
	IP A	ddress		
Server Fingerprints	Hops Primary/Secondary	Generic List Block Type (31)		
mgerprints	Generic List Block Type, continued	Generic List Block Length		
	Generic List Block Length, continued	Server Fingerprint Data Blocks*		
Client Fingerprints	Generic List E	Block Type (31)		
mgerprints	Generic List	Block Length		
	Client Fingerpr	int Data Blocks*		
SMB Fingerprints	Generic List F	Block Type (31)		
i ingerprints	Generic List	Block Length		
	SMB Fingerprint Data Blocks*			
DHCP Fingerprints	Generic List E			
i ingerprints	Generic List			
	DHCP Fingerpi			
	List Block	List of TCP Servers		
	List Blo	200,000		
TCP Server Block*	Server Bloo			
	Server Block Length			
	TCP Ser			
	List Block	List of UDP Servers		
	List Blo			
UDP Server Block*	Server Bloc			
	Server Blo	ock Length		
	UDP Ser	ver Data		

Byte	0	1	2	3		
Bit	0 1 2 3 4 5 6 7					
		List Block	Type (11)		List of Network	
		List Bloc	k Length		Protocols	
Network Protocol		Protocol Blo	ck Type (4)*			
Block*		Protocol Bl	ock Length			
		Network Pro	tocol Data			
		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 Block Length					
MAC Address Block*	MAC Address Block Type (95)*					
		MAC Address Block Length				
	MAC Address Data					
	Host Last Seen					
	Host Type					
	VLAN Presence	VLA	N ID	VLAN Type		
	VLAN Priority	AN Priority Generic List Block Type (31)		List of Client Applications		
	Generic List Block Type, continued	G	eneric List Block Le	ngth		
Client App Data	Generic List Block Length, continued	Client A	Application Block Ty	/pe (112)*		
	Client App Block Type (29)*, con't					
	Client Application Block Length, con't	C	lient Application Da	ta		

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		
NetBIOS Name	String Block Type (0)		
ranic	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-31 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-157 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.	

Table B-31 Host Profile Data Block for 5.0 - 5.0.2 Fields (continued)

Field	Data Type	Description	
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-157 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 for 5.0 - 5.0.2, page B-157 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-157 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.	

Table B-31 Host Profile Data Block for 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 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).	
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 4-75.	
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 4-75.	
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-31 Host Profile Data Block for 5.0 - 5.0.2 Fields (continued)

Field	Data Type	Description	
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 4-115.	
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)	
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 4-156.	
String Block Type	uint32	Initiates a string data block for the NetBIOS name. This value is set to 0 to indicate string data.	

Table B-31 Host Profile Data Block for 5.0 - 5.0.2 Fields (continued)

Field	Data Type	Description
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-157

#### **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.

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 2 2 2 2 2 2 2 2		
	Operating System Fingerprint Block Type (87)		
	Operating System Fingerprint Block Length		
OS Fingerprint	Fingerprint UUID		
UUID	Fingerprint UUID, continued		
	Fingerprint UUID, continued		
	Fingerprint UUID, continued		
	Fingerprint Type		
	Fingerprint Source Type		
	Fingerprint Source ID		
	Last Seen Value for Fingerprint		
	TTL Difference		

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

Table B-32 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.
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-159
- Connection Statistics Data Block 5.1, page B-163
- Connection Statistics Data Block 5.2.x, page B-169
- Connection Chunk Data Block for 5.0 5.1, page B-175
- Connection Chunk Data Block for 5.1.1-6.0.x, page B-176
- Connection Statistics Data Block 5.1.1.x, page B-178
- Connection Statistics Data Block 5.3, page B-184
- Connection Statistics Data Block 5.3.1, page B-191
- Connection Statistics Data Block 5.4, page B-198
- Connection Statistics Data Block 5.4.1, page B-211
- Connection Statistics Data Block 6.0.x, page B-224
- Connection Statistics Data Block 6.1.x, page B-239
- Connection Statistics Data Block 6.2-6.7.x, page B-256

• Connection Statistics Data Block 7.0, page B-272

## **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 4-53.

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

•		
•		

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 2 2 2 2 2			
	Connection Data Block Type (115)			
	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			

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				
		Initiator IP Add	ress, continued		
		Initiator IP Add	ress, continued		
		Initiator IP Adda	ress, continued		
		Responder I	IP Address		
		Responder IP Add	dress, continued		
		Responder IP Add	dress, continued		
		Responder IP Add	dress, continued		
		Policy R	evision		
		Policy Revision	on, continued		
		Policy Revision, continued			
	Policy Revision, continued				
		Rule	ID		
		Rule A	Action		
	Initiator Port Responder Port				
	TCP	Flags	Protocol	NetFlow Source	
		NetFlow Source			
		NetFlow Source			
	NetFlow Source, continued				
		etFlow Source, continue		First Pkt Time	
		Packet Timestamp, cont		Last Pkt Time	
	Last F	Packet Timestamp, conti		Packets Sent	
		Packets Sent		D 1 ( D 1	
		Packets Sent, continued		Packets Rcvd	
		Packets Receiv		D C	
	Pac	ckets Received, continu	ea	Bytes Sent	

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       6     7     8     9     0     1     2     3	2 2 2 2 2 3 3 4 5 6 7 8 9 0 1		
	Bytes Sent, continued				
	Packets Received, continue	ed	Bytes Rcvd		
	Bytes Received	d, continued			
	Bytes Received, continued	d	User ID		
	User ID, continued		Application Protocol ID		
	Application Protocol ID, conti	inued	URL Category		
	URL Category, continued	i	URL Reputation		
	URL Reputation, continued Client App ID				
	Client Application ID, continued Web App ID				
	Web Application ID, continued  String Bloc (0)				
Client App URL	String Block Type, continue	String Block Length			
	String Block Length, continu	Client Application URL			
NetBIOS Name	String Block Type (0)				
rvanic	String Block Length				
	NetBIOS N	Name			
Client App Version	String Block Type (0)				
Tipp version	String Block Length				
	Client Application Version				

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

Table B-33 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.	
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.	

Table B-33 Connection Statistics Data Block 5.0 - 5.0.2 Fields (continued)

Field	Data Type	Description		
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.		

# **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 4-53.

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

::

Byte	0	1	2	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					
	Connection Data Block Type (126)						
	Connection Data Block Length						
		Device ID					
		Ingres	s Zone				
		Ingress Zor	e, continued				
		Ingress Zor	e, continued				
		Ingress Zor	e, continued				
		Egres	s Zone				
		Egress Zon	e, continued				
		Egress Zone, continued					
	Egress Zone, continued						
	Ingress Interface						
	Ingress Interface, continued						
		Ingress Interface, continued					
		Ingress Interface, continued					
	Egress Interface						
		Egress Interface, continued					
		Egress Interf	ace, continued				
		Egress Interf	ace, continued				
		Initiator l	P Address				
		Initiator IP Ad	dress, continued				
		Initiator IP Ad	dress, continued				
		Initiator IP Ad	dress, continued				
		Responder	IP Address				
		Responder IP A	ddress, 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 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		
	Responder IP Address, continued					
		Responder IP Ad	dress, continued			
	Policy Revision					
		Policy Revision	on, continued			
		Policy Revision	on, continued			
		Policy Revision	on, continued			
		Rule	ID			
	Rule A	Action	Rule R	Reason		
	Initiator Port Responder Port					
	TCP I	Flags	Protocol	NetFlow Source		
		NetFlow Sour	ce, continued			
	NetFlow Source, continued					
	NetFlow Source, continued					
	Ne	etFlow Source, continue	ed	First Pkt Time		
	First P	Packet Timestamp, cont	inued	Last Pkt Time		
	Last Packet Timestamp, continued  Initiator Transmitted Packets					
		Initiator Transmitted	Packets, continued			
	Initiator Transmitted Packets, continued  Responder Transmitted Packets					
	Responder Transmitted Packets, continued					
	Responder Transmitted Packets, continued  Initiator Transmitted Bytes					
		Initiator Transmitte	d Bytes, continued			
	Initiator	Transmitted Bytes, con	ntinued	Responder Transmitted Bytes		
		Responder Transmitt	ed Bytes, continued			

Byte	0	1	2	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			
	Responder Transmitted Bytes, continued User II				
	User ID, continued Application Protocol ID				
	Applic	cation Protocol ID, cor	ntinued	URL Category	
	U	RL Category, continue	ed	URL Reputation	
	UF	RL Reputation, continu	ıed	Client App ID	
	Clien	t Application ID, cont	inued	Web App ID	
	Web	Application ID, conti	nued	String Block Type (0)	
Client App URL	Stri	ng Block Type, contin	ued	String Block Length	
	String Block Length, continued  Client Application URL			Client Application URL	
NetBIOS Name		String Blo	ck Type (0)		
Tunic	String Block Length				
	NetBIOS Name				
Client App Version	String Block Type (0)				
	String Block Length				
	Client Application Version				
		Monito	r Rule 1		
		Monito	r Rule 2		
	Monitor Rule 3				
	Monitor Rule 4				
	Monitor Rule 5				
			r Rule 6		
			r Rule 7		
	G 1 . G 5		r 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-34 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.	
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.	

Table B-34 Connection Statistics Data Block 5.1 Fields (continued)

Field	Data Type	Description		
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.		
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.		

Table B-34 Connection Statistics Data Block 5.1 Fields (continued)

Field	Data Type	Description
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 block list.
Security Intelligence Layer	uint8	The IP layer that matched the IP block list.

### **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-178.

For more information on the Connection Statistics Data message, see Connection Statistics Data Message, page 4-53.

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 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 Data Block Type (144)			
	Connection Data Block Length				
	Device ID				
	Ingress Zone				
	Ingress Zone, continued				
	Ingress Zone, continued				
	Ingress Zone, continued				
		Egress	Zone		

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		
	Egress Zone, continued					
		Egress Zone, continued				
		Egress Zone	, continued			
		Ingress I	nterface			
		Ingress Interfa	ce, continued			
		Ingress Interfa	ce, continued			
		Ingress Interfa	ce, continued			
		Egress I	nterface			
		Egress Interfa	ce, continued			
		Egress Interfa	ce, 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 Ad	dress, continued			
		Policy R	evision			
		Policy Revision	on, continued			
		Policy Revision	on, continued			
		Policy Revision	on, continued			
		Rule	ID			
	Rule A	Action	Rule I	Reason		
	Initiato	or Port	Respon	der Port		

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     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		
	TCP Flags Protocol			NetFlow Source		
		NetFlow Sour	ce, continued			
		NetFlow Sour	ce, continued			
		NetFlow Sour	ce, continued			
	Ne	etFlow Source, continue	ed	Instance ID		
	Instance ID, cont.	Connectio	n Counter	First Pkt Time		
	First P	acket Timestamp, cont	inued	Last Pkt Time		
	Last P	acket Timestamp, cont	inued	Initiator Tx Packets		
		Initiator Transmitted Packets, continued				
	Initiator Transmitted Packets, continued			Resp. Tx Packets		
	Responder Transmitted Packets, continued Initiator Tx Bytes					
		Initiator Transmitte	d Bytes, continued			
	Initiator	Resp. Tx Bytes				
	Responder Transmitted Bytes, continued					
	Responde	User ID				
	User ID, continued Application ID					
	Applic	URL Category				
	U	RL Category, continue	d	URL Reputation		
	URL Reputation, continued			Client App ID		
	Clien	t Application ID, conti	nued	Web App ID		
Client URL	Web	Application ID, contin	nued	Str. Block Type (0)		
	Stri	ng Block Type, continu	ued	String Block Length		
	Strin	g Block Length, contir	nued	Client App. 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 Block Type (0)					
Tvarie		String Bloo	ck Length			
		NetBIOS Name				
Client App Version		String Bloc	k Type (0)			
Tipp voision		String Bloo	ck Length			
		Client Application 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					
	Intrusion E	vent Count	Initiator	Country		
	Responder Country					

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

Table B-35 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.

Table B-35 Connection Statistics Data Block 5.2.x Fields (continued)

Field	Data Type	Description		
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.		
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.		

Table B-35 Connection Statistics Data Block 5.2.x Fields (continued)

Field	Data Type	Description			
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 byte for the string block type and length fields, plus the number objects 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.			

Table B-35 Connection Statistics Data Block 5.2.x Fields (continued)

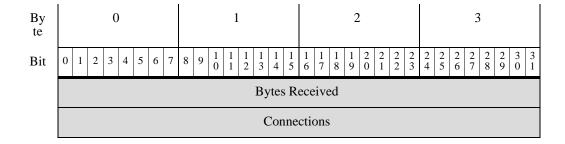
Field	Data Type	Description
Monitor Rule 8	uint32	The ID of the eighth monitor rule associated with the connection event.
Security Intelligence Source/ Destination	uint8	Whether the source or destination IP address matched the IP block list.
Security Intelligence Layer	uint8	The IP layer that matched the IP block list.
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 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 Chui	nk Block Length			
		Initiator II	P Address			
		Responder	IP Address			
		Start '	Time			
		Applica	tion ID			
	Respond	ler Port	Protocol	Connection Type		
	NetFlow Detector IP Address					
	Packets Sent					
	Packets Received					
	Bytes Sent					



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

Table B-36 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.			
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 Chunk Data Block for 5.1.1-6.0.x**

The Connection Chunk data block conveys connection data. It stores connection log data that aggregates over a five-minute period. The Connection Chunk data block has a block type of 136 in the series 1 group of blocks. It supersedes block type 119.

The following diagram shows the format of the Connection Chunk 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				
		Connection Chunk Block Type (136)						
	Connection Chunk Block Length							
		Initiator IP Address						
		Responder l	IP Address					
		Start 7	Гіте					
		Application	n Protocol					
	Responder Port Protocol Connection Type							
	NetFlow Detector IP Address							
	Packets Sent							
	Packets Sent, continued							
	Packets Received							
	Packets Received, continued							
	Bytes Sent							
	Bytes Sent, continued							
	Bytes Received							
	Bytes Received, continued							
		Connec	ctions					

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

Table B-37 Connection Chunk Data Block Fields

Field	Data Type	Description
Connection Chunk Block Type	uint32	Initiates a Connection Chunk data block. This value is always 136.
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 initiator of this type of connection. This is used with the responder IP address to identify identical connections.

Table B-37 Connection Chunk Data Block Fields (continued)

Field	Data Type	Description	
Responder IP Address	uint8(4)	IP address of the responder to this type of connection. This is used with the initiator IP address to identify identical connections.	
Start Time	uint32	The starting time for the connection chunk.	
Application Protocol	uint32	Identification number for the protocol used in the connection.	
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.	
NetFlow Detector IP Address	uint8[4]	IP address of the NetFlow device that detected the connection, in IP address octets.	
Packets Sent	uint64	The number of packets sent in the connection chunk.	
Packets Received	uint64	The number of packets received in the connection chunk.	
Bytes Sent	uint64	The number of bytes sent in the connection chunk.	
Bytes Received	uint64	The number of bytes received in the connection chunk.	
Connections	uint32	The number of connections over a five-minute period.	

#### **Connection Statistics Data Block 5.1.1.x**

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-163.

For more information on the Connection Statistics Data message, see Connection Statistics Data Message, page 4-53.

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

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		
	Connection Data Block Type (137)					
	Connection Data Block Length					
	Device ID					
	Ingress Zone					
	Ingress Zone, continued					
	Ingress Zone, continued					
		Ingress Zone	e, continued			

Byte	0	1			2			3	
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1	$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	$\begin{array}{c cc} 1 & 1 & 1 \\ 6 & 7 & 8 \end{array}$	$\begin{array}{c cc} 1 & 2 & 2 \\ 9 & 0 & 1 \end{array}$	$\begin{bmatrix} 2 & 2 \\ 2 & 3 \end{bmatrix}$	2 2 2 4 5 6	2 2 7 8	$\begin{array}{c cc} 2 & 3 & 3 \\ 9 & 0 & 1 \end{array}$
	Egress Zone Egress Zone, continued								
	Egress Zone, continued								
	Egress Zone, continued								
			Ingress I	nterface					
		Ingr	ess Interfa	ice, conti	inued				
		Ingr	ess Interfa	ice, conti	inued				
		Ingr	ess Interfa	ice, conti	inued				
			Egress I	nterface					
		Egr	ess Interfa	ce, conti	nued				
		Egr	ess Interfa	ce, conti	nued				
	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								
		Kespoi			minued				
	Policy Revision								
	Policy Revision, continued								
	Policy Revision, continued  Policy Revision, continued								
		1 01	Rule						
	Rule A	Action	21010		F	Rule R	Reason		

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	$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	2     2     2     2     2     2     3     3       4     5     6     7     8     9     0     1		
	Initiat	ler Port				
	TCP	NetFlow Source				
		NetFlow Sour	ce, continued			
		NetFlow Sour	ce, continued			
		NetFlow Sour	ce, continued			
	No	etFlow Source, continue	ed	Instance ID		
	Instance ID, cont.	Connection	n Counter	First Pkt Time		
	First I	Packet Timestamp, cont	inued	Last Pkt Time		
	Last I	Packet Timestamp, cont	inued	Initiator Tx Packets		
		Initiator Transmitted	Packets, continued			
	Initiator	Initiator Transmitted Packets, continued				
	Responder Transmitted Packets, continued					
	Responde	Initiator Tx Bytes				
	Initiator Transmitted Bytes, continued					
	Initiato	Resp. Tx Bytes				
		Responder Transmitt	ed Bytes, continued			
	Respond	er Transmitted Bytes, c	ontinued	User ID		
		Application Prot. ID				
	Applio	cation Protocol ID, cont	tinued	URL Category		
	U	JRL Category, continue	d	URL Reputation		
	Ul	Client App ID				
	Clier	Web App ID				
Client URL	Web	Str. Block Type (0)				
- <del></del>	Stri	String Block Length				
	Striı	ng Block Length, contin	nued	Client App. URL		

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 2 3 4 5 6 7 8 9 0 1 3 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1					
NetBIOS Name	String Block Type (0)						
1 (1111)		String Blo	ck Length				
		NetBIOS	Name				
Client App Version		String Block Type (0)					
T-FF * * * * * * * * * * * * * * * * * *		String Blo	ck Length				
	Client Application 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 Eve	ent Count			
	Intrusion Event Count						

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

Table B-38 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, 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.

Table B-38 Connection Statistics Data Block 5.1.1.x Fields (continued)

Field	Data Type	Description	
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.	
User ID	uint32	Internal identification number for the user who last logged into the host that generated the traffic.	

Table B-38 Connection Statistics Data Block 5.1.1.x Fields (continued)

Field	Data Type	Description			
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.			
Monitor Rule 6	uint32	The ID of the sixth monitor rule associated with the connection event.			

Table B-38 Connection Statistics Data Block 5.1.1.x Fields (continued)

Field	Data Type	Description
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 block list.
Security Intelligence Layer	uint8	The IP layer that matched the IP block list.
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**

Byte

Bit

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-169.

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 2-13. 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 4-53.

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

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

Byte	0	1				2				3		
Bit	0 1 2 3 4 5 6 7	8 9 1 1	1 1 1 2 3 4	1 6	1 1 7 8	$\begin{bmatrix} 1 & 2 \\ 9 & 0 \end{bmatrix}$	2 2 2 1 2 3	2 4	2 2 5 6	2 7	2 2 8 9	3 3 0 1
	Egress Zone											
		]	Egress Zo	ie, co	ontinu	ued						
		]	Egress Zo	ie, co	ontinu	ued						
		]	Egress Zo	ie, co	ontinu	ued						
			Ingress	Inter	rface							
		Ing	gress Inter	face,	conti	inued						
		Ing	gress Inter	ace,	cont	inued						
		Ing	gress Inter	face,	cont	inued						
			Egress	Inter	face							
		Eg	ress Inter	ace,	conti	nued						
	Egress Interface, continued											
	Egress Interface, continued											
			Initiator	IP A	ddres	SS						
			ator IP Ac									
			ator IP Ac									
			ator IP Ac									
	Responder IP Address continued											
	Responder IP Address, continued											
	Responder IP Address, continued											
	Responder IP Address, continued											
	Policy Revision  Policy Revision, continued											
	Policy Revision, continued  Policy Revision, continued											
	Policy Revision, continued											
				le ID								
	Rule A	action					Rule I	Rea	son			

Bit    O   1   2   3   4   5   6   7   8   9   0   1   2   1   1   1   1   1   1   1   1	Byte	0	1	2	3		
NetFlow Source, continued Instance ID Instance ID, cont. Connection Counter First Pkt Time Last Packet Timestamp, continued Initiator Transmitted Packets, continued Initiator Transmitted Packets, continued Initiator Transmitted Packets, continued Responder Transmitted Packets, continued Responder Transmitted Bytes, continued Initiator Transmitted Bytes,	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		
NetFlow Source, continued NetFlow Source, continued NetFlow Source, continued NetFlow Source, continued Instance ID Instance ID, cont. Connection Counter First Packet Timestamp, continued Last Pkt Time Last Packet Timestamp, continued Initiator Tx Packets Initiator Transmitted Packets, continued Responder Transmitted Packets, continued Responder Transmitted Packets, continued Initiator Transmitted Bytes, continued Responder Transmitted Bytes, continued Initiator 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 Client Application ID, continued URL String Block Type, continued String Block Type, continued String Block Type, continued String Block Type, continued String Block Length		Initiat	or Port	Respond	ler Port		
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  Responder Transmitted Packets, continued  Responder Transmitted Packets, continued  Responder Transmitted Bytes, continued  Initiator Transmitted Bytes, continued  Responder Transmitted Bytes, continued  Initiator Transmitted Bytes, continued  Responder Transmitted Bytes, continued  Responder Transmitted Bytes, continued  Responder Transmitted Bytes, continued  Responder Transmitted Bytes, continued  User ID  Application Protocol ID, continued  URL Category  URL Category, continued  URL Reputation  URL Reputation  URL Reputation  Client Application ID, continued  Str. Block Type (0)  String Block Length		ТСР	Flags	Protocol	NetFlow Source		
NetFlow Source, continued  NetFlow Source, continued  Instance ID  Instance ID, cont.  Connection Counter  First Packet Time  First Packet Timestamp, continued  Last Pkt Time  Last Packet Timestamp, continued  Initiator Trax  Packets  Initiator Transmitted Packets, continued  Initiator Transmitted Packets, continued  Responder Transmitted Packets, continued  Initiator Transmitted Bytes, continued  Initiator Transmitted Bytes, continued  Responder Transmitted Bytes, continued  Responder Transmitted Bytes, continued  Interval Bytes  Responder Transmitted Bytes, continued  Responder Transmitted Bytes, continued  User ID  User ID, continued  URL Category  URL Category, continued  URL Reputation  URL Reputation  Client App ID  Client Application ID, continued  Str. Block Type (0)  String Block Type, continued  String Block Type, continued			NetFlow Source	ce, continued			
Instance ID, cont.  Connection Counter  First Pkt Time  First Packet Timestamp, continued  Last Pkt Time  Last Packet Timestamp, continued  Initiator Transmitted Packets, continued  Initiator Transmitted Packets, continued  Responder Transmitted Packets, continued  Responder Transmitted Packets, continued  Initiator Transmitted Packets, continued  Responder Transmitted Bytes, continued  Initiator Transmitted Bytes, continued  Responder Transmitted Bytes, continued  Responder Transmitted Bytes, continued  Responder Transmitted Bytes, continued  User ID  Application Prot. ID  Application Prot. ID  Application Prot. ID  Client Application ID, continued  Client App ID  Client Application ID, continued  Str. Block Type (0)  String Block Type, continued  String Block Length			NetFlow Source	ce, continued			
Instance ID, cont.  Connection Counter  First Pkt Time  Last Packet Timestamp, continued  Last Pkt Time  Last Packet Timestamp, continued  Initiator Tx Packets  Initiator Transmitted Packets, continued  Resp. Tx Packets  Responder Transmitted Packets, continued  Responder Transmitted Packets, continued  Initiator Transmitted Packets, continued  Responder Transmitted Bytes, continued  Initiator Transmitted Bytes, continued  Responder Transmitted Bytes, continued  Responder Transmitted Bytes, continued  Responder Transmitted Bytes, continued  Responder Transmitted Bytes, continued  User ID  User ID, continued  URL Category  URL Category, continued  URL Reputation  URL Reputation  Client App ID  Client Application ID, continued  Web Application ID, continued  Client Web Application ID, continued  Str. Block Type (0)  String Block Length			NetFlow Source	ce, continued			
First Packet Timestamp, continued  Last Packet Timestamp, continued  Initiator Transmitted Packets, continued  Initiator Transmitted Packets, continued  Resp. Tx Packets  Responder Transmitted Packets, continued  Responder Transmitted Packets, continued  Initiator Tx Bytes  Initiator Transmitted Bytes, continued  Responder Transmitted Bytes, continued  Responder 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  Client App ID  Client Application ID, continued  Str. Block Type (0)  String Block  Length		Ne	etFlow Source, continue	ed	Instance ID		
Last Packet Timestamp, continued  Initiator Transmitted Packets, continued  Initiator Transmitted Packets, continued  Responder Transmitted Packets, continued  Responder Transmitted Packets, continued  Initiator Transmitted Packets, continued  Responder Transmitted Bytes, continued  Initiator Transmitted Bytes, continued  Responder Transmitted Bytes, continued  Responder Transmitted Bytes, continued  Responder Transmitted Bytes, continued  User ID  User ID  Application Protocol ID, continued  URL Category  URL Category, continued  URL Reputation  URL Reputation  Client App ID  Client Application ID, continued  Str. Block Type (0)  String Block  Length		Instance ID, cont.	Connection	n Counter	First Pkt Time		
Initiator Transmitted Packets, continued  Initiator Transmitted Packets, continued  Responder Transmitted Packets, continued  Responder Transmitted Packets, continued  Initiator Transmitted Packets, continued  Initiator Transmitted Bytes, continued  Initiator Transmitted Bytes, continued  Responder Transmitted Bytes, continued  Responder Transmitted Bytes, continued  Initiator Transmitted Bytes  Initiator Transmited Bytes  Initiator Transmited Bytes  Initiator Transmited Bytes  Initiat		First I	Packet Timestamp, cont	inued	Last Pkt Time		
Initiator Transmitted Packets, continued Responder Transmitted Packets, continued Responder Transmitted Packets, continued 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 Client Application ID, continued URL String Block Type, continued String Block Length		Last F	Packet Timestamp, conti	inued			
Responder Transmitted Packets, continued Responder Transmitted Packets, continued 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 Prot. ID  URL Category URL Category URL Reputation URL Reputation URL Reputation URL Reputation URL Reputation ID, continued URL Reputation ID, continued URL Reputation URL Reputation ID, continued URL Reputation URL Reputation ID, continued URL Reputation URL Reputation ID, continued URL Reputation		Initiator Transmitted Packets, continued					
Responder Transmitted Packets, continued  Initiator Transmitted Bytes, continued  Initiator Transmitted Bytes, continued  Resp. Tx Bytes  Responder 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  Client App ID  Client  Web App ID  Client  Web Application ID, continued  Str. Block Type (0)  String Block  Length		Initiator Transmitted Packets, continued Resp. Tx Packets					
Initiator Transmitted Bytes, continued  Initiator Transmitted Bytes, continued  Responder Transmitted Bytes, continued  Responder Transmitted Bytes, continued  User ID  User ID, continued  Application Prot.  ID  Application Prot.  URL Category  URL Category, continued  URL Reputation		Responder Transmitted Packets, continued					
Initiator Transmitted Bytes, continued  Responder 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  URL Reputation  URL App ID  Client App ID  Client URL  String Block Type, continued  String Block Length		Responde	r Transmitted Packets, o	continued	Initiator Tx Bytes		
Responder 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  Str. Block Type (0)  String Block Length			Initiator Transmitted	d 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  Client App ID  Client Application ID, continued  Web App ID  Client URL  String Block Type, continued  Str. Block Type (0)  String Block Length		Initiator	r Transmitted Bytes, con	ntinued	Resp. Tx Bytes		
User ID, continued  Application Prot. ID  Application Protocol ID, continued  URL Category  URL Category, continued  URL Reputation  URL Reputation  URL Reputation  Client App ID  Client Application ID, continued  Web App ID  Client Web Application ID, continued  Str. Block Type (0)  String Block Length			Responder Transmitt	ed Bytes, continued			
Application Protocol ID, continued  URL Category  URL Category, continued  URL Reputation  URL Reputation  Client App ID  Client Application ID, continued  Web App ID  Client URL  String Block Type, continued  Str. Block Type (0)  String Block Length		Respond	er Transmitted Bytes, co	ontinued	User ID		
URL Category, continued  URL Reputation  URL Reputation  Client App ID  Client Application ID, continued  Web App ID  Client URL  Web Application ID, continued  Str. Block Type (0)  String Block Type, continued  String Block Length							
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  String Block Length		Application Protocol ID, continued URL Category					
Client Application ID, continued Web App ID  Client URL  String Block Type, continued  Str. Block Type (0)  String Block Length		URL Category, continued URL Reputation					
Client URL  String Block Type, continued  Str. Block Type (0)  String Block Length		URL Reputation, continued Client App ID					
URL String Block Type, continued String Block Length		Client Application ID, continued Web App ID					
Length		Web	Application ID, contin	ued	Str. Block Type (0)		
String Block Length, continued Client App. URL		Stri	ing Block Type, continu	ued			
		Strir	ng Block Length, contin	ued	Client App. 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	$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	2 2 2 2 2 3 3 4 5 6 7 8 9 0 1			
NetBIOS		String Bloc	ck Type (0)				
Name		String Blo	ck Length				
		NetBIOS	Name				
Client App Version		String Bloc	ek Type (0)				
App 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						
	Intrusion Event Count Initiator Country						
	Responder Country IOC Number						
	Source Autonomous System						
	Destination Autonomous 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-39 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-39 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-39 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 block list.			
Security Intelligence Layer	uint8	The IP layer that matched the IP block list.			
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-39 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-184.

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 2-13. 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 4-53.

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

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										
		Connection Data I	Block Type (154)											
		Connection Data	a Block Length											
		Devic	ee 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 I	nterface											
	Ingress Interface, continued													
	Ingress Interface, continued													
	Ingress Interface, continued													

Byte	0		1					2						3	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	1 9	2 2	2	2 2 3	2 2 4	2 2 5	2 7	2 2 9	3 3 0 1
				Egre	ess I	nte	rface									
			Egre	ss In	terfa	ice,	cont	inue	d							
			Egre	ss In	terfa	ice,	cont	inue	d							
			Egre	ss In	terfa	ice,	cont	inue	d							
			Iı	nitiat	or I	P A	ddres	SS								
	Initiator IP Address, continued  Initiator IP Address, continued  Initiator IP Address, continued															
			Re	espon	der	IP A	Addr	ess								
		Re	spon	der II	P Ac	ldre	ess, co	onti	nue	d						
		Re	spon	der II	P Ac	ldre	ess, co	onti	nue	d						
		Re	spon	der II	P Ac	ldre	ess, co	onti	nue	d						
				Poli	cy F	Revi	ision									
			Polic	y Re	visi	on,	conti	nue	d							
			Polic	y Re	visi	on,	conti	nue	d							
			Polic	y Re	visi	on,	conti	nue	d							
					Rul	e ID	)									
	Rule A	ction											ison			
	Initiato	r Port							F	Res	spoi	ndei	Port			
	TCP I	Flags					P	roto	col				NetF	low	Sou	rce
			NetF	low S	Sou	rce,	cont	inue	ed							
			NetF	low S	Sou	rce,	cont	inue	ed							
	NetFlow Source, continued															
	NetFlow Source, continued Instance ID															
	Instance ID, cont. Connection Counter First Pkt Time															
	First P	acket Ti	mesta	amp,	con	tinu	ied						Las	t Pk	t Tin	ne

Byte		0					1						2			Î			3			ĺ
Bit	0 1 2	2 3 4	5 6	7	8 9	1 1 0 1	1 2	1 1 3 4	1 5	1 6	1 7	1 8 9	2 0	2 2	2	2 2 4	$\begin{bmatrix} 2 & 2 & 2 \\ 4 & 5 & 6 \end{bmatrix}$	2 2	2 2 2 7 8	2 2 9	3	3
			Las	st P	acket	Tim	estar	np, c	ont	inu	ed								ato: cke	r Tx ets		
					Init	tiator	Trai	nsmi	tted	Pa	.cke	ets, c	conti	nue	d							
		]	Initiat	or [	Гrans	mitte	ed Pa	cket	s, co	onti	nu	ed					Resp	). T	`x F	Pack	ets	
					Resp	ond	er Tr	ansn	itte	d P	Pacl	xets,	con	tinu	iec	l						
		R	espon	der	Tran	smit	ted P	acke	ts,	con	tin	ued					Initia	itoi	: T	к Ву	tes	
		Initiator Transmitted Bytes, continued  Initiator Transmitted Bytes, continued																				
			Initia	tor													Res	p. '	Tx	Byte	es	
						_	ler T				-		cont	inue	ed	Г						
			Respo	nde						ont	ınu	ed							er l			
					Use	r ID,	cont	inue	a								App		ID	n Pi	οι.	
			App	olic	ation	Prot	ocol	ID, o	ont	inu	ed						UR	LO	Cat	egoi	у	
				U	RL C	atego	ory, c	conti	nue	d							URI	R	epı	ıtati	on	
				UR	L Re	puta	tion,	cont	inu	ed							Cli	ent	A	op II	D	
			Cl	ien	t App	licat	ion I	D, co	nti	nue	d						W	eb	Ap	p IE	)	
Client URL			W	/eb	Appl	icati	on II	), co	ntin	uec	1						Str. B	loc	k T	Гуре	(0)	)
			S	Strii	ng Bl	ock '	Гуре	, con	tinı	ied									g B eng	lock		
			St	trin	g Blo	ck L	engtl	n, co	ntin	uec	1					-	Clien	t A	pp.	. UR	L	
NetBIOS Name							Stri	ng B	loc	k T	ур	e (0)										
							Str	ring 1	3lo	ck I	Len	gth										
								[etB]														
Client App Version								ng B			_											
						- CI		ring ]														
						Cl	ient .						n									
								Mon Mon														
								IVIOII	itUf	ΙΝU	116.	۷										

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-40 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-40 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 TransmittedBytes	uint64	Number of bytes transmitted by the initiating host.
Responder Transmitted Bytes	uint64	Number of bytes transmitted by the responding host.

Table B-40 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-40 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 block list.
Security Intelligence Layer	uint8	The IP layer that matched the IP block list.
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.

## **Connection Statistics Data Block 5.4**

The connection statistics data block is used in connection data messages. Several new fields have been added to the Connection Statistics Data Block for 5.4. Fields have been added to support SSL connections, HTTP redirection, and network analysis policies. The connection statistics data block for version 5.4 has a block type of 155 in the series 1 group of blocks. It deprecates block type 154, Connection Statistics Data Block 5.3.1, page B-191.

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 12 and an event code of 71. See Request Flags, page 2-13. 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 4-53.

The following diagram shows the format of a Connection Statistics data block for 5.4:

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									
		Connection Data I	Block Type (155)										
	Connection Data Block Length												
	Device 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 I	nterface										
		Ingress Interfa	ce, continued										
		Ingress Interfa	ce, continued										
	Ingress Interface, continued												
		Egress I	nterface										
	Egress Interface, continued												

Byte	0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 3													2								3	3									
Bit	0 1	2	3	4	5	6	7	8	9	10		1 2	1 1 3	1 4	1 5	1	1 7		1 1	0		2	2 2	2 3	2 4	2 5	6	2 7	2 8	2 9	3	3
										]	Eg	ŗe	ess l	nte	rfa	ce	e, co	on	ntin	ıed												
										]	Eg	gre	ess l	nte	rfa	ce	e, co	on	ntin	ıed												
												]	Initi	ato	r II	Ρ.	Add	lre	ess													
	Initiator IP Address, continued																															
	Initiator IP Address, continued																															
	Initiator IP Address, continued																															
	Responder IP Address																															
	Responder IP Address, continued																															
	Responder IP Address, continued																															
									]	Res	pc	on	der	ΙP	Ad	ldı	ress	, (	con	tinı	ue	ed										
													Po	olic	y R	Re <sup>*</sup>	visi	OI	n													
													cy I																			
													cy I																			
											Po	li	cy I					n	tinı	ied												
														R	ule	e I	D															
							ıle A																		lea							
							tiato														]	Re	sp	one	1		ort					
						T	CP I	Fla	gs		_								Pro			1				N	etF	low	/ S	our	ce	
													Flov																			
													Flov																			
													Flov					on	itin	ıed	ļ									-		
								tFl	ow	Sc	ur		e, co														Ins					
	Instance ID, cont. Connection Counter First Pkt Time																															
	First Packet Timestamp, continued  Last Pkt Time  Last Packet Timestamp, continued  Initiator Tx																															
						∟a	st P	ack	cet	Tir	ne	st	amp	o, c	ont	un	ued	1										tiat Pacl				

Byte	0	1			2	2					3			
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 3	1 1 4 5	1 1 6 7	1 1 8 9	2 0	2 2 2	2 3	2 2 4 5	2 6	2 2 7 8	2 9		3
		Initiator Transm	ittec	l Pack	ets, c	ont	inue	d						
	Initiator '	Fransmitted Packe	ts, c	ontinu	ied				Re	sp. ˈ	Тх Р	ack	ets	
		Responder Trans	mitte	ed Pac	kets,	cor	ntinu	ed						
	Responder		Initiator Tx Bytes											
	Initiator	Re	esp.	Tx I	Byte	es								
	Responde	er Transmitted Byt	es, c	ontin	ıed					U	ser II	D		
		User ID, continu	ed						Ap	plic	ation ID	ı Pr	ot.	
	Applic	ation Protocol ID,	con	tinued	l				U	RL	Cate	gor	у	
	U	RL Category, cont	inue	d					UF	RL I	Repu	tatio	on	
	UF	RL Reputation, cor	tinu	ed					C	lien	ıt Ap	p II	)	
	Clien	t Application ID,	conti	nued					7	Web	App	D	)	
	Web	Application ID, c	ontir	nued					Str.	Blo	ck T	ype	(0)	
Client URL	Stri	ng Block Type, co	ntin	ued					S		ng Bl engtl			
	Strin	g Block Length, c	ontir	nued					Clie	nt A	App.	UR	L	
S		String	Bloc	k Typ	e (0)									
NetBIOS Name		String	Blo	ck Le	ngth									
Ž		NetE	SIOS	Nam	e									
ion		String	Bloc	k Typ	e (0)									
Client App Version		String	Blo	ck Le	ngth									
App														
	Monitor Rule 1													
		Mo	nitoi	Rule	2									
		Mo	nitor	Rule	3									

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											
		Monitor	Rule 4												
		Monitor	Rule 5												
		Monitor	tor Rule 6												
		Monitor	tor Rule 7												
		Monitor	itor Rule 8												
	Sec. Int. Src/Dst	Sec. Int. Layer	File Eve	nt Count											
	Intrusion E	vent Count	Initiator	Country											
	Responde	r Country	IOC N	umber											
		Source Autono	omous System												
		Destination Auto	onomous System												
	SNM	IP In	SNM	P Out											
	Source TOS	Destination TOS	Source Mask Destination Mask												
		Security	y Context												
		Security Conto	ntext, continued												
		-	ntext, continued												
			ntext, continued												
ced Host	VLA		String Bloc												
	String Block Typ		String Blo												
Referen	String Block Le	ngth, continued	Referenced Host												
ıt		String Bloc	lock Type (0)												
User Agent		String Blo	Block Length												
Use		User A	r Agent												
rer		String Bloc	Block Type (0)												
Refer		String Blo	Block Length												
HTTP Referrer		HTTP R	eferrer												
H															

Byte	0	1	I				2					3				
Bit	0 1 2 3 4 5 6 7	8 9 1 1		1 1		1 1 8		2 2	2 2 3	2 4	2 2 5 6	2 7	2 8 9	3 3 0 1		
		SS	L Cert	ific	ate Fir	gerp	rint									
		SSL Cer	rtificate	Fi	ngerpi	int, c	onti	inued	l							
		SSL Cer	rtificate	Fi	ngerpi	int, c	onti	inued	l							
		SSL Cer	rtificate	Fi	ngerpi	int, c	onti	inued	l							
		SSL Cer	rtificate	Fi	ngerpi	int, c	onti	inued	l							
			SS	L P	olicy l	D										
	SSL Policy ID, continued															
	SSL Policy ID, continued															
	SSL Policy ID, continued															
	SSL Rule ID															
	SSL Cipher Suite SSL Version SSL Srv Cert. S															
	SSL Srv Cert. Stat., cont.		SSL .	Act	tual Ac	tion				SSL Expected Action						
	SSL Expected Action, cont.		SSL	Flo	ow Sta	tus					SSL	Flo	w En	ror		
	SS	L Flow Err	or, con	tinı	ued								Flow ages			
	SSL	Flow Mess	ages, c	ont	inued						SSL	Flo	w Fla	ags		
		SS	SL Flov	/ Fl	lags, co	ontin	ied			-						
ames	SS	L Flow Fla	ıgs, con	tinı	ued					S	tring	Blo (0	ock T	ype		
SSL Server Names	String	g Block Typ	pe (0), o	con	tinued						String Block Length					
SST S	Strin	g Block Le	ngth, c	ont	inued							L S Vam	ervei ie	r		
			SSL U	JRI	L Cate	gory										
	SSL Session ID															
		SS	SL Sess	ion	ID, co	ontinu	ied									
		SS	SL Sess	ion	ID, co	ontinu	ied									

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										
		SSL Session I	D, continued											
	SSL Session ID, continued													
	SSL Session ID, continued													
	SSL Session ID, continued													
	SSL Session ID, continued													
	SSL Session ID Length SSL Ticket ID													
		SSL Ticket I	D, continued											
		SSL Ticket I	D, continued											
		SSL Ticket I	D, continued											
		SSL Ticket I	D, continued											
	SSL Ticket ID, cont.	SSL Ticket ID Length	Network Analysis	s Policy Revision										
	1	Network Analysis Police	cy Revision, continued	1										
	1	Network Analysis Polic	cy Revision, continued											
	I	Network Analysis Police	cy Revision, continued	1										
	Network Analysis conti													

The following table describes the fields of the Connection Statistics data block for 5.4+.

Table B-41 Connection Statistics Data Block 5.4+ Fields

Field	Data Type	Description
Connection Statistics Data Block Type	uint32	Initiates a Connection Statistics data block for 5.4+. The value is always 155.
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-41 Connection Statistics Data Block 5.4+ 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-41 Connection Statistics Data Block 5.4+ 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-41 Connection Statistics Data Block 5.4+ 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 block list.
Security Intelligence Layer	uint8	The IP layer that matched the IP block list.
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.
VLAN ID	uint16	VLAN identification number that indicates which VLAN the host is a member of.
String Block Type	uint32	Initiates a String data block containing the Referenced Host. This value is always 0.
String Block Length	uint32	The number of bytes included in the Referenced Host String data block, including eight bytes for the block type and header fields plus the number of bytes in the Referenced Host field.

Table B-41 Connection Statistics Data Block 5.4+ Fields (continued)

Field	Data Type	Description								
Referenced Host	string	Host name information provided in HTTP or DNS.								
String Block Type	uint32	Initiates a String data block containing the User Agent. This value is always 0.								
String Block Length	uint32	The number of bytes included in the User Agent String data block, including eight bytes for the block type and header fields plus the number of bytes in the User Agent field.								
User Agent	string	Information from the UserAgent header field in the session.								
String Block Type	uint32	Initiates a String data block containing the HTTP Referrer. This value is always 0.								
String Block Length	uint32	The number of bytes included in the HTTP Referrer String data block, including eight bytes for the block type and header fields plus the number of bytes in the HTTP Referrer field.								
HTTP Referrer	string	The site from which a page originated. This is found int he Referred header information in HTTP traffic.								
SSL Certificate Fingerprint	uint8[20]	SHA1 hash of the SSL Server certificate.								
SSL Policy ID	uint8[16]	ID number of the SSL policy that handled the connection.								
SSL Rule ID	uint32	ID number of the SSL rule or default action that handled the connection.								
SSL Cipher Suite	uint16	Encryption suite used by the SSL connection. The value is stored in decimal format. See www.iana.org/assignments/tls-parameters/tls-parameters.xhtml for the cipher suite designated by the value.								
SSL Version	uint8	The SSL or TLS protocol version used to encrypt the connection.								
SSL Server	uint16	The status of the SSL certificate. Possible values include:								
Certificate Status		• 0 — Not checked — The server certificate status was not evaluated.								
		• 1 — Unknown — The server certificate status could not be determined.								
		• 2 — Valid — The server certificate is valid.								
		• 4 — Self-signed — The server certificate is self-signed.								
		• 16 — Invalid Issuer — The server certificate has an invalid issuer.								
		• 32 — Invalid Signature — The server certificate has an invalid signature.								
		• 64 — Expired — The server certificate is expired.								
		• 128 — Not valid yet — The server certificate is not yet valid.								
		• 256 — Revoked — The server certificate has been revoked.								

Table B-41 Connection Statistics Data Block 5.4+ Fields (continued)

Field	Data Type	Description
SSL Actual Action	uint16	The action performed on the connection based on the SSL Rule. This may differ from the expected action, as the action as specified in the rule may be impossible. Possible values include:
		• 0 — 'Unknown'
		• 1 — 'Do Not Decrypt'
		• 2 — 'Block'
		• 3 — 'Block With Reset'
		• 4 — 'Decrypt (Known Key)'
		• 5 — 'Decrypt (Replace Key)'
		• 6 — 'Decrypt (Resign)'
SSL Expected Action	uint16	The action which should be performed on the connection based on the SSL Rule. Possible values include:
		• 0 — 'Unknown'
		• 1 — 'Do Not Decrypt'
		• 2 — 'Block'
		• 3 — 'Block With Reset'
		• 4 — 'Decrypt (Known Key)'
		• 5 — 'Decrypt (Replace Key)'
		• 6 — 'Decrypt (Resign)'

Table B-41 Connection Statistics Data Block 5.4+ Fields (continued)

Field	Data Type	Description
SSL Flow Status	uint16	Status of the SSL Flow. These values describe the reason
		behind the action taken or the error message seen. Possible
		values include:
		• 0 — 'Unknown'
		• 1 — 'No Match'
		• 2 — 'Success'
		• 3 — 'Uncached Session'
		• 4 — 'Unknown Cipher Suite'
		• 5 — 'Unsupported Cipher Suite'
		• 6 — 'Unsupported SSL Version'
		• 7 — 'SSL Compression Used'
		• 8 — 'Session Undecryptable in Passive Mode'
		• 9 — 'Handshake Error'
		• 10 — 'Decryption Error'
		• 11 — 'Pending Server Name Category Lookup'
		• 12 — 'Pending Common Name Category Lookup'
		• 13 — 'Internal Error'
		• 14 — 'Network Parameters Unavailable'
		• 15 — 'Invalid Server Certificate Handle'
		• 16 — 'Server Certificate Fingerprint Unavailable'
		• 17 — 'Cannot Cache Subject DN'
		• 18 — 'Cannot Cache Issuer DN'
		• 19 — 'Unknown SSL Version'
		• 20 — 'External Certificate List Unavailable'
		• 21 — 'External Certificate Fingerprint Unavailable'
		• 22 — 'Internal Certificate List Invalid'
		• 23 — 'Internal Certificate List Unavailable'
		• 24 — 'Internal Certificate Unavailable'
		• 25 — 'Internal Certificate Fingerprint Unavailable'
		• 26 — 'Server Certificate Validation Unavailable'
		• 27 — 'Server Certificate Validation Failure'
		• 28 — 'Invalid Action'
SSL Flow Error	uint32	Detailed SSL error code. These values may be needed for support purposes.

Table B-41 Connection Statistics Data Block 5.4+ Fields (continued)

Field	Data Type	Description
SSL Flow Messages	uint32	The messages exchanged between client and server during the SSL handshake. See http://tools.ietf.org/html/rfc5246 for more information.
		• 0x00000001 — NSE_MTHELLO_REQUEST
		• 0x00000002 — NSE_MTCLIENT_ALERT
		• 0x00000004 — NSE_MTSERVER_ALERT
		• 0x00000008 — NSE_MTCLIENT_HELLO
		• 0x00000010 — NSE_MTSERVER_HELLO
		• 0x00000020 — NSE_MTSERVER_CERTIFICATE
		• 0x00000040 — NSE_MTSERVER_KEY_EXCHANGE
		• 0x00000080 — NSE_MTCERTIFICATE_REQUEST
		• 0x00000100 — NSE_MTSERVER_HELLO_DONE
		• 0x00000200 — NSE_MTCLIENT_CERTIFICATE
		• 0x00000400 — NSE_MTCLIENT_KEY_EXCHANGE
		• 0x00000800 — NSE_MTCERTIFICATE_VERIFY
		• 0x00001000 — NSE_MTCLIENT_CHANGE_CIPHER_SPEC
		• 0x00002000 — NSE_MTCLIENT_FINISHED
		• 0x00004000 — NSE_MTSERVER_CHANGE_CIPHER_SPEC
		• 0x00008000 — NSE_MTSERVER_FINISHED
		• 0x00010000 — NSE_MTNEW_SESSION_TICKET
		• 0x00020000 — NSE_MTHANDSHAKE_OTHER
		• 0x00040000 — NSE_MTAPP_DATA_FROM_CLIENT
		• 0x00080000 — NSE_MTAPP_DATA_FROM_SERVER
SSL Flow Flags	uint64	The debugging level flags for an encrypted connection. Possible values include:
		0x00000001 — NSE_FLOWVALID - must be set for other fields to be valid
		• 0x00000002 — NSE_FLOWINITIALIZED - internal structures ready for processing
		0x00000004 — NSE_FLOWINTERCEPT - SSL session has been intercepted
String Block Type	uint32	Initiates a String data block containing the SSL Server Name. This value is always o.

Field	Data Type	Description
String Block Length	uint32	The number of bytes included in the SSL Server Name String data block, including eight bytes for the block type and header fields plus the number of bytes in the SSL Server Name field.
SSL Server Name	string	Name provided in the server name indication in the SSL Client Hello.
SSL URL Category	uint32	Category of the flow as identified from the server name and certificate common name.
SSL Session ID	uint8[32]	Value of the session ID used during the SSL handshake when the client and server agree to do session reuse
SSL Session ID Length	uint8	Length of the SSL Session ID. While the session ID cannot exceed 32 bytes, it may be less than 32 bytes.
SSL Ticket ID	uint8[20]	Hash of the session ticket used when the client and server agree to use a session ticket.
SSL Ticket ID Length	uint8	Length of the SSL Ticket ID. While the ticket ID cannot exceed 20 bytes, it may be less than 20 bytes.
Network Analysis Policy revision	uint8[16]	Revision of the Network Analysis Policy associated with the connection event.

Table B-41 Connection Statistics Data Block 5.4+ Fields (continued)

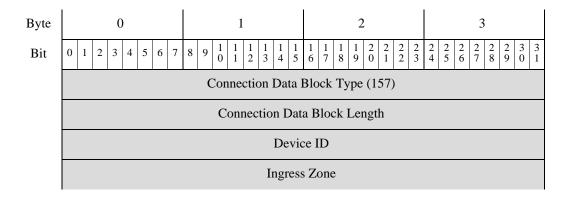
## **Connection Statistics Data Block 5.4.1**

The connection statistics data block is used in connection data messages. Several new fields have been added to the Connection Statistics Data Block for 5.4. Fields have been added to support SSL connections, HTTP redirection, and network analysis policies. The connection statistics data block for version 5.4+ has a block type of 157 in the series 1 group of blocks. It deprecates block type 155, Connection Statistics Data Block 5.3.1, page B-191.

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 12 and an event code of 71. See Request Flags, page 2-13. 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 4-53.

The following diagram shows the format of a Connection Statistics data block for 5.4+:



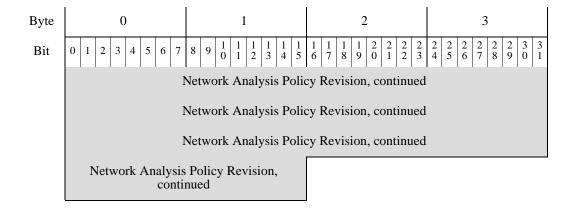
Byte	0	1	2		3										
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 4	$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	$\begin{array}{c ccc} 2 & 2 & 2 \\ 1 & 2 & 3 \end{array}$	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1										
		Ingress Z	one, continued	' '											
		Ingress Z	one, continued												
		Ingress Z	one, continued												
	Egress Zone														
	Egress Zone, continued														
	Egress Zone, continued														
	Egress Zone, continued														
	Ingress Interface														
	Ingress Interface, continued														
	Ingress Interface, continued														
			erface, continued												
			ss Interface												
			erface, continued												
			erface, continued												
			erface, continued												
			r IP Address	1											
			Address, continue												
			Address, continue												
			ler IP Address	<u> </u>											
			Address, continu	ed											
		_	Address, continu												
		_	Address, continu												
			y Revision												
		Policy Rev	rision, continued												
		Policy Rev	rision, continued												

Byte	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 1 6 7	1 8	1 1			2 2	2 2 3	4	2 4	2 2 5		2 7	2 2 2	3	3		
			.,	Po	lic	y R	evi	sic	n, co	nt	tinı	ied		·							,	·			
							Rı	ule	ID																
	Rule Action Rule I													Reason											
	Initiator Port Respond												de	er I	Port										
	TCP	Flag	;s							I	Pro	toc	ol			NetFlow Source									
				Ne	tFl	low	So	ur	ce, co	n	tin	ued				-									
	NetFlow Source, continued																								
	NetFlow Source, continued																								
	Ne	tFlo	w S	Sour	ce,	, coi	ntiı	าน	ed									In	sta	anc	e II	)			
	Instance ID, cont.				C	onn	ect	ioı	ı Cou	ın	ter							Firs	t I	Pkt	Tir	ne			
	First F	ack	et T	'ime	sta	mp,	, co	ont	inued	l							Last Pkt Time								
	Last P	ack	et T	ime	sta	mp,	cc	nt	inued	]							Initiator Tx Packets								
		Ir	nitia	tor '	Tra	ansn	nitt	ted	Pack	cet	ts,	con	tiı	nue	d										
	Initiator	Гrar	ısm	itted	l Pa	acke	ets,	, co	ntinu	ıe	d					Resp. Tx Packets						S			
		Re	spo	ndeı	Tı	rans	mi	tte	d Pac	ck	ets	, co	nt	inu	ied										
	Responde	Tra	ansr	nitte	ed I	Pacl	ket	s, c	conti	ıu	ied					Initiator Tx Bytes							s		
		]	[niti	ator	Tr	ans	mi	tte	d Byt	es	s, c	onti	in	uec	l										
	Initiator	Tra	nsn	nitte	d E	Byte	es,	COI	ntinu	ed	l						I	Res	p. ˈ	Tx	Ву	tes			
		R	espo	onde	er T	Γran	sn	itt	ed By	yte	es,	con	ıti	nue	ed										
	Responde	er Tı	rans	mitt	ted	Ву	tes	, c	ontin	ue	ed							1	Us	er	ID				
	User ID, continued											A	ppl		atio ID	on F	rot	•							
	Application Protocol ID, continued												,	UR.	L (	Ca	tego	ry							
	U	RL	Cate	egoi	y,	con	tin	ue	d								ι	JRL	R	lep	utat	ion	l		
	UF	RL F	Repu	ıtati	on,	, coi	nti	nue	ed									Clie	ent	t A	.pp ]	D			
	Clien	t Ap	plio	catio	on l	ID,	COI	ntiı	nued									We	eb	Aj	pp I	D			

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	
	Web Application ID, continued Str. Block Type (6				
Client	String Block Type, continued			String Block Length	
	String Block Length, continued			Client App. URL	
S	String Block Type (0)				
NetBIOS Name	String Block Length				
	NetBIOS Name				
ion	String Block Type (0)				
Client App Version	String Block Length				
App	Client Application 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 Ever	nt Count	
	Intrusion Event Count  Responder Country		Initiator Country		
			IOC Number		
	Source Autonomous System				
		onomous System			
	SNMP In		SNMP Out		
	Source TOS	Destination TOS	Source Mask	Destination Mask	
	Security Context				

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		
	Security Context, continued					
	Security Context, continued					
	Security Context, continued					
Referenced Host	VLA	N ID	String Bloc	ek Type (0)		
	String Block Typ	pe (0), continued	String Blo	ck Length		
	String Block Length, continued		Referenced Host			
ent	String Block Type (0)					
User Agent	String Block Length					
nso	User Agent					
errer	String Block Type (0)					
HTTP Referrer	String Block Length					
HTT	HTTP Referrer					
	SSL Certificate Fingerprint					
	SSL Certificate Fingerprint, continued					
	SSL Certificate Fingerprint, continued					
	SSL Certificate Fingerprint, continued					
	SSL Certificate Fingerprint, continued					
	SSL Policy ID					
	SSL Policy ID, continued					
	SSL Policy ID, continued					
	SSL Policy ID, continued					
	SSL Rule ID					
	SSL Cipl	SSL Version	SSL Srv Cert. Stat.			
	SSL Srv Cert. Stat., cont.			SSL Actual Action		
	SSL Actual Action, cont.	SSL Flow Status				

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     1     2     3     3       6     7     8     9     0     0     1     2     3     4     5     6     7     8     9     0	3	
	SSL Flow Status, SSL Flow Error cont.		SSL Flow Error		
	SSL Flow Error, cont.	SSL Flow Messages			
	SSL Flow Msg. Cont.		SSL Flow Flags		
		SSL Flow Fla	ngs, continued		
SSL Server Names	SSL Flow Flags, continued		String Block Type (0)		
	String Block Type (0), continued		String Block Length		
SSFS	String Block Length, continued		SSL Server Name		
		SSL URL	Category		
	SSL Session ID				
	SSL Session ID, continued				
	SSL Session ID, continued				
	SSL Session ID, continued				
		SSL Session l	ID, continued		
	SSL Session ID, continued				
	SSL Session ID, continued				
	SSL Session ID, continued  SSL Session ID Length  SSL Ticket ID				
	SSL Ticket ID, continued				
	SSL Ticket ID, continued				
	SSL Ticket ID, continued				
	SSL Ticket ID, continued				
	SSL Ticket ID, cont.	SSL Ticket ID Length	Network Analysis Policy Revision		



The following table describes the fields of the Connection Statistics data block for 5.4+.

Table B-42 Connection Statistics Data Block 5.4+ Fields

Field	Data Type	Description								
Connection Statistics Data Block Type	uint32	Initiates a Connection Statistics data block for 5.4+. The value is always 157.								
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.								

Table B-42 Connection Statistics Data Block 5.4+ Fields (continued)

Field	Data Type	Description									
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.									
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.									

Table B-42 Connection Statistics Data Block 5.4+ Fields (continued)

Field	Data Type	Description
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 block list.
Security Intelligence Layer	uint8	The IP layer that matched the IP block list.
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.

Table B-42 Connection Statistics Data Block 5.4+ Fields (continued)

Field	Data Type	Description								
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.								
VLAN ID	uint16	VLAN identification number that indicates which VLAN the host is a member of.								
String Block Type	uint32	Initiates a String data block containing the Referenced Host. This value is always 0.								
String Block Length	uint32	The number of bytes included in the Referenced Host String data block, including eight bytes for the block type and header fields plus the number of bytes in the Referenced Host field.								
Referenced Host	string	Host name information provided in HTTP or DNS.								
String Block Type	uint32	Initiates a String data block containing the User Agent. This value is always 0.								
String Block Length	uint32	The number of bytes included in the User Agent String data block, including eight bytes for the block type and header fields plus the number of bytes in the User Agent field.								
User Agent	string	Information from the UserAgent header field in the session.								
String Block Type	uint32	Initiates a String data block containing the HTTP Referrer. This value is always 0.								
String Block Length	uint32	The number of bytes included in the HTTP Referrer String data block, including eight bytes for the block type and header fields plus the number of bytes in the HTTP Referrer field.								
HTTP Referrer	string	The site from which a page originated. This is found int he Referred header information in HTTP traffic.								
SSL Certificate Fingerprint	uint8[20]	SHA1 hash of the SSL Server certificate.								
SSL Policy ID	uint8[16]	ID number of the SSL policy that handled the connection.								
SSL Rule ID	uint32	ID number of the SSL rule or default action that handled the connection.								

Table B-42 Connection Statistics Data Block 5.4+ Fields (continued)

Field	Data Type	Description
SSL Cipher Suite	uint16	Encryption suite used by the SSL connection. The value is stored in decimal format. See www.iana.org/assignments/tls-parameters/tls-parameters. xhtml for the cipher suite designated by the value.
SSL Version	uint8	The SSL or TLS protocol version used to encrypt the connection.
SSL Server	uint32	The status of the SSL certificate. Possible values include:
Certificate Status		• 0 — Not checked — The server certificate status was not evaluated.
		• 1 — Unknown — The server certificate status could not be determined.
		• 2 — Valid — The server certificate is valid.
		• 4 — Self-signed — The server certificate is self-signed.
		• 16 — Invalid Issuer — The server certificate has an invalid issuer.
		• 32 — Invalid Signature — The server certificate has an invalid signature.
		• 64 — Expired — The server certificate is expired.
		• 128 — Not valid yet — The server certificate is not yet valid.
		• 256 — Revoked — The server certificate has been revoked.
SSL Actual Action	uint16	The action performed on the connection based on the SSL Rule. This may differ from the expected action, as the action as specified in the rule may be impossible. Possible values include:
		• 0 — 'Unknown'
		• 1 — 'Do Not Decrypt'
		• 2 — 'Block'
		• 3 — 'Block With Reset'
		• 4 — 'Decrypt (Known Key)'
		• 5 — 'Decrypt (Replace Key)'
		• 6 — 'Decrypt (Resign)'
SSL Expected Action	uint16	The action which should be performed on the connection based on the SSL Rule. Possible values include:
		• 0 — 'Unknown'
		• 1 — 'Do Not Decrypt'
		• 2 — 'Block'
		• 3 — 'Block With Reset'
		• 4 — 'Decrypt (Known Key)'
		• 5 — 'Decrypt (Replace Key)'
		• 6 — 'Decrypt (Resign)'

Table B-42 Connection Statistics Data Block 5.4+ Fields (continued)

Field	Data Type	Description
SSL Flow Status	uint16	Status of the SSL Flow. These values describe the reason
		behind the action taken or the error message seen. Possible
		values include:
		<ul><li>0 — 'Unknown'</li><li>1 — 'No Match'</li></ul>
		• 2 — 'Success'
		• 3 — 'Uncached Session'
		• 4 — 'Unknown Cipher Suite'
		• 5 — 'Unsupported Cipher Suite'
		• 6 — 'Unsupported SSL Version'
		• 7 — 'SSL Compression Used'
		• 8 — 'Session Undecryptable in Passive Mode'
		• 9 — 'Handshake Error'
		• 10 — 'Decryption Error'
		• 11 — 'Pending Server Name Category Lookup'
		• 12 — 'Pending Common Name Category Lookup'
		• 13 — 'Internal Error'
		• 14 — 'Network Parameters Unavailable'
		• 15 — 'Invalid Server Certificate Handle'
		• 16 — 'Server Certificate Fingerprint Unavailable'
		• 17 — 'Cannot Cache Subject DN'
		• 18 — 'Cannot Cache Issuer DN'
		• 19 — 'Unknown SSL Version'
		• 20 — 'External Certificate List Unavailable'
		• 21 — 'External Certificate Fingerprint Unavailable'
		• 22 — 'Internal Certificate List Invalid'
		• 23 — 'Internal Certificate List Unavailable'
		• 24 — 'Internal Certificate Unavailable'
		• 25 — 'Internal Certificate Fingerprint Unavailable'
		• 26 — 'Server Certificate Validation Unavailable'
		• 27 — 'Server Certificate Validation Failure'
		• 28 — 'Invalid Action'
SSL Flow Error	uint32	Detailed SSL error code. These values may be needed for support purposes.

Table B-42 Connection Statistics Data Block 5.4+ Fields (continued)

Field	Data Type	Description								
SSL Flow Messages	uint32	The messages exchanged between client and server during the SSL handshake. See http://tools.ietf.org/html/rfc5246 for more information.								
		• 0x00000001 — NSE_MTHELLO_REQUEST								
		• 0x00000002 — NSE_MTCLIENT_ALERT								
		• 0x00000004 — NSE_MTSERVER_ALERT								
		• 0x00000008 — NSE_MTCLIENT_HELLO								
		• 0x00000010 — NSE_MTSERVER_HELLO								
		• 0x00000020 — NSE_MTSERVER_CERTIFICATE								
		• 0x00000040 — NSE_MTSERVER_KEY_EXCHANGE								
		• 0x00000080 — NSE_MTCERTIFICATE_REQUEST								
		• 0x00000100 — NSE_MTSERVER_HELLO_DONE								
		• 0x00000200 — NSE_MTCLIENT_CERTIFICATE								
		• 0x00000400 — NSE_MTCLIENT_KEY_EXCHANGE								
		• 0x00000800 — NSE_MTCERTIFICATE_VERIFY								
		• 0x00001000 —  NSE_MTCLIENT_CHANGE_CIPHER_SPEC								
		• 0x00002000 — NSE_MTCLIENT_FINISHED								
		• 0x00004000 —  NSE_MTSERVER_CHANGE_CIPHER_SPEC								
		• 0x00008000 — NSE_MTSERVER_FINISHED								
		• 0x00010000 — NSE_MTNEW_SESSION_TICKET								
		• 0x00020000 — NSE_MTHANDSHAKE_OTHER								
		• 0x00040000 — NSE_MTAPP_DATA_FROM_CLIENT								
		• 0x00080000 — NSE_MTAPP_DATA_FROM_SERVER								
SSL Flow Flags	uint64	The debugging level flags for an encrypted connection. Possible values include:								
		0x00000001 — NSE_FLOWVALID - must be set for other fields to be valid								
		0x00000002 — NSE_FLOWINITIALIZED - internal structures ready for processing								
		0x00000004 — NSE_FLOWINTERCEPT - SSL session has been intercepted								
String Block Type	uint32	Initiates a String data block containing the SSL Server Name. This value is always 0.								

Table B-42 Connection Statistics Data Block 5.4+ Fields (continued)

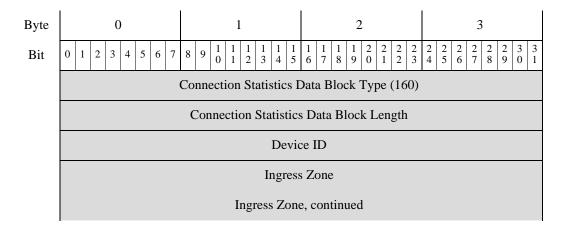
Field	Data Type	Description								
String Block Length	uint32	The number of bytes included in the SSL Server Name String data block, including eight bytes for the block type and header fields plus the number of bytes in the SSL Server Name field.								
SSL Server Name	string	Name provided in the server name indication in the SSL Client Hello.								
SSL URL Category	uint32	Category of the flow as identified from the server name and certificate common name.								
SSL Session ID	uint8[32]	Value of the session ID used during the SSL handshake when the client and server agree to do session reuse								
SSL Session ID Length	uint8	Length of the SSL Session ID. While the session ID cannot exceed 32 bytes, it may be less than 32 bytes.								
SSL Ticket ID	uint8[20]	Hash of the session ticket used when the client and server agree to use a session ticket.								
SSL Ticket ID Length	uint8	Length of the SSL Ticket ID. While the ticket ID cannot exceed 20 bytes, it may be less than 20 bytes.								
Network Analysis Policy revision	uint8[16]	Revision of the Network Analysis Policy associated with the connection event.								

## **Connection Statistics Data Block 6.0.x**

The connection statistics data block is used in connection data messages. Several new fields have been added to the Connection Statistics Data Block for 6.0. Fields have been added to support ISE Integration and Multiple Network Maps. The connection statistics data block for version 6.0.x has a block type of 160 in the series 1 group of blocks. It supersedes block type 157, Connection Statistics Data Block 5.4.1, page B-211. New fields have been added to support DNS lookup and Security Intelligence.

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 13 and an event code of 71. See Request Flags, page 2-13. If you enable bit 23, an extended event header is included in the record.

The following diagram shows the format of a Connection Statistics data block for 6.0.x:



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 3 4 5 6 7 8 9 0 1										
		Ingress Zon	e, continued											
		Ingress Zon	e, continued											
		Egres	s Zone											
		Egress Zon	e, continued											
	Egress Zone, continued  Egress Zone, continued													
	Ingress Interface													
	Ingress Interface, continued  Ingress Interface, continued													
	Ingress Interface, continued													
		Egress l	Interface											
		Egress Interfa	ace, continued											
		Egress Interfa	ace, continued											
			ace, continued											
			P Address											
			dress, continued											
			dress, continued											
			dress, continued											
			IP Address											
		_	ddress, continued											
		_	ddress, continued											
			ddress, continued											
			Revision											
			ion, continued											
			ion, continued											
		Policy Revisi	ion, continued											

Byte	0								1								2							3								
Bit	0 1	2	3	3 4	5	6	5 7	8	ç	9 1			1 1 2				1 1 6 7			1 2 9 0	2	2 2	2	2 4	2	2 2 6	7	2 2 2 3			3	
														F	Ru	ıle I	ID															
					I	Rι	ule A	Act	io	n											F	Rule	R	lea	sc	n						
				I	Rule	e l	Rea	son	١,	con	t.						Initiator Port															
					Re	es]	pon	der	P	ort							TCP Flags															
		P	ro	toc	ol												Ne	etl	Flo	w S	our	ce										
		NetFlow Source, continued																														
		NetFlow Source, continued																														
	NetFlow Source, continued																															
	Net	Flo	w	Sro	c, c	or	nt.		Instance ID																			n				
	Cx Counter, cont. First Packet Timestamp																															
	F	irst		kt T ont.	im	e,	•	Last Packet Timestamp																								
	L	ast		kt T ont.	`im	e,			Initiator Transmitted Packets																							
								]	n	itia	tor	T	ran	smi	tte	ed l	Pack	κe	ts,	con	tinu	ied										
	In	itia		r Ta	x Pl	kt	•							R	.es	spo	nde	r ′	Tra	nsm	itte	ed F	ac	ke	ts							
								R	es	spo	nde	r	Tra	nsn	nit	tted	l Pac	ck	ets	s, co	ntir	nue	l									
	Res	. T	<b>x</b> ]	Pkt	s, c	or	nt.								I	niti	iator	. ]	Гrа	nsm	itte	d B	yt	es								
									I	niti	atoı	. "	Trai	ısm	it	ted	Byt	te	s, c	conti	nue	ed										
	In			r Tz ont.	кВ	ts	,							]	Re	esp	onde	er	Tı	ansı	nitt	ted	Ву	/tes	S							
								F	Re	espo	ond	eı	r Tr	ansı	m	itte	d B	yt	es,	con	tinı	ued										
	Re	s. T	'x	Bts	, cc	on	ıt.												Us	er II	)											
	Use	r II	Э,	con	ntin	u	ed									A	pplic	ca	tio	n Pr	oto	col	ID	)								
	Ap	p P	ro	t ID	), co	on	nt.										U	R	L	Cate	goı	у										
	U	RL		Cate ont.	gor	y,	,										UF	RI	L R	lepu	tati	on										

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 2 2 2 2 2 2 2 2 2 3 3 3 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1											
	URL Rep, cont.		Client Application ID											
	Client App ID, cont.		Web Application ID											
	Web App ID, cont.	2	String. Block Type (0)											
Client URL	Str. Block Type, cont.	String Block Length												
	Str. Block Len., cont.	Client App. URL												
S		String Bloc	k Type (0)											
NetBIOS Name		String Bloo	ck Length											
Z		NetBIOS	Name											
t		String Block Type (0)												
Client App Version		String Bloo	ck Length											
Apl		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											
	Intrusion E	vent Count	Initiator Country											
	Responder	r Country	IOC Number											
		Source Autono	omous System											
		Destination Auto	onomous System											
	SNM	P In	SNMP Out											

Byte	0	1					2			3					
Bit	0 1 2 3 4 5 6 7		$\begin{array}{c cccc} 1 & 1 & 1 \\ 2 & 3 & 4 \end{array}$	1 5	1 1 6 7	1 8	1 2 9 0	2	2 2 2 3	2 4	2 2 5 6	2 7	2 8 9	3 3 0 1	
	Source TOS	Destination	on TOS		Source Mask Destination Mask								ask		
			Securi	ty	Cont	ext									
		Seco	urity Co	nte	ext, co	onti	nued								
	Security Context, continued  Security Context, continued														
Host	VLAN ID String Block Type (0)														
ced F	String Block Typ	e (0), contin	ued				St	tring	g Blo	ck l	Leng	th			
Referenced Host	String Block Le	ngth, continu	ued				F	Refe	erenc	ed F	Host.	•			
sut	String Block Type (0)														
User Agent	String Block Length														
Use			User	A	gent.										
rrer		S	String Bl	oc	k Typ	pe ((	0)								
Refe		;	String B	lo	ck Le	ngtl	n								
HTTP Referrer			HTTP	R	eferre	r									
		SSI	. Certifi	cat	te Fin	gerj	print								
		SSL Cert	ificate F	in	gerpr	int,	conti	inue	ed						
		SSL Cert	ificate F	in	gerpr	int,	conti	inue	ed						
		SSL Cert	ificate F	in	gerpr	int,	conti	inue	ed						
		SSL Cert	ificate F	in	gerpr	int,	conti	inue	d						
			SSL	Po	licy I	D									
		SS	L Policy	/ <b>I</b> ]	D, co	ntin	ued								
		SS	L Policy	/ <b>I</b> ]	D, co	ntin	ued								
		SS	L Policy	/ []	D, co	ntin	ued								
			SSL	R	ule II	)									
	SSL Cipl	er Suite			5	SSL	Vers	sion		SS	SL S	rv C	ert. S	Stat.	

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 2 2 2 2 2	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1									
	S	SL Srv Cert. Stat., cont.	SSL Actual Action									
	SSL actual Action cont.	SSL Expected Action	SSL Flow Status									
	SSL Flow Status, cont.	SSL Flow Error										
	SSL Flow Error, cont.	SSL Flow Messages										
	SSL Flow Msg, cont.	SSL Flow Flags										
		SSL Flow Flags, cont.										
ames	SSL Flow Flags, continued	String Block Type (0)										
SSL Server Names	String Block Type (0), continued	String Block Length										
SSF S	String Block Length, continued	SSL Server Name										
		SSL URL Category										
		SSL Session ID										
		SSL Session ID, continued										
		SSL Session ID, continued										
		SSL Session ID, continued										
		SSL Session ID, continued										
		SSL Session ID, continued										
		SSL Session ID, continued										
		SSL Session ID, continued										
	SSL Session ID Length	SSL Ticket ID										
		SSL Ticket ID, continued										
		SSL Ticket ID, continued										
		SSL Ticket ID, 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 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								
		SSL Ticket II	D, continued									
	SSL Ticket ID, cont.	SSL Ticket ID Length	Network Analysis	ork Analysis Policy Revision								
	1	Metwork Analysis Policy Revision, continued										
	1	Network Analysis Police	cy Revision, continued									
	I	Network Analysis Polic	cy Revision, continued									
	Network Analysis conti		Endpoint 1	Profile ID								
	Endpoint Profile	e ID, continued	Security (	Group ID								
	Security Group	ID, continued	Location	on IPv6								
	Location IPv6, continued											
		Location IPv	6, continued									
		Location IPv	6, continued									
	Location IPv	6, continued	HTTP Response									
	HTTP Respon	se, continued	String Block Type (0)									
	String Block Typ	be (0), continued	String Block Length									
	String Block Le	ngth, continued	DNS Query									
	DNS Rec	ord Type	DNS Response Type									
		DNS	TTL									
		Sinkhole	e UUID									
		Sinkhole UUI	D, continued									
		Sinkhole UUI	TID, continued									
		Sinkhole UUI	D, continued									
		Security Intell	ligence List 1									
		Security Intell	ligence List 2									

The following table describes the fields of the Connection Statistics data block for 6.0.x.

Table B-43 Connection Statistics Data Block 6.0.x Fields

Field	Data Type	Description
Connection Statistics Data Block Type	uint32	Initiates a Connection Statistics data block for 6.0+. The value is always 160.
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	uint32	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-43 Connection Statistics Data Block 6.0.x 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-43 Connection Statistics Data Block 6.0.x 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 block list.								
Security Intelligence Layer	uint8	The IP layer that matched the IP block list.								
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.								

Table B-43 Connection Statistics Data Block 6.0.x Fields (continued)

Field	Data Type	Description
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.
VLAN ID	uint16	VLAN identification number that indicates which VLAN the host is a member of.
String Block Type	uint32	Initiates a String data block containing the Referenced Host. This value is always 0.
String Block Length	uint32	The number of bytes included in the Referenced Host String data block, including eight bytes for the block type and header fields plus the number of bytes in the Referenced Host field.
Referenced Host	string	Host name information provided in HTTP or DNS.
String Block Type	uint32	Initiates a String data block containing the User Agent. This value is always 0.
String Block Length	uint32	The number of bytes included in the User Agent String data block, including eight bytes for the block type and header fields plus the number of bytes in the User Agent field.
User Agent	string	Information from the UserAgent header field in the session.
String Block Type	uint32	Initiates a String data block containing the HTTP Referrer. This value is always 0.
String Block Length	uint32	The number of bytes included in the HTTP Referrer String data block, including eight bytes for the block type and header fields plus the number of bytes in the HTTP Referrer field.
HTTP Referrer	string	The site from which a page originated. This is found int he Referred header information in HTTP traffic.
SSL Certificate Fingerprint	uint8[20]	SHA1 hash of the SSL Server certificate.
SSL Policy ID	uint8[16]	ID number of the SSL policy that handled the connection.
SSL Rule ID	uint32	ID number of the SSL rule or default action that handled the connection.
SSL Cipher Suite	uint16	Encryption suite used by the SSL connection. The value is stored in decimal format. See  www.iana.org/assignments/tls-parameters/tls-parameters.  xhtml for the cipher suite designated by the value.
SSL Version	uint8	The SSL or TLS protocol version used to encrypt the connection.

Table B-43 Connection Statistics Data Block 6.0.x Fields (continued)

Field	Data Type	Description							
SSL Server	uint32	The status of the SSL certificate. Possible values include:							
Certificate Status		• 0 — Not checked — The server certificate status was not evaluated.							
		• 1 — Unknown — The server certificate status could not be determined.							
		• 2 — Valid — The server certificate is valid.							
		• 4 — Self-signed — The server certificate is self-signed.							
		• 16 — Invalid Issuer — The server certificate has an invalid issuer.							
		• 32 — Invalid Signature — The server certificate has an invalid signature.							
		• 64 — Expired — The server certificate is expired.							
		• 128 — Not valid yet — The server certificate is not yet valid.							
		• 256 — Revoked — The server certificate has been revoked.							
SSL Actual Action	uint16	The action performed on the connection based on the SSL Rule.  This may differ from the expected action, as the action as specified in the rule may be impossible. Possible values include:  • 0 — 'Unknown'							
		• 0 — 'Unknown'							
		• 1 — 'Do Not Decrypt'							
		• 2 — 'Block'							
		• 3 — 'Block With Reset'							
		• 4 — 'Decrypt (Known Key)'							
		• 5 — 'Decrypt (Replace Key)'							
		• 6 — 'Decrypt (Resign)'							
SSL Expected Action	uint16	The action which should be performed on the connection based on the SSL Rule. Possible values include:							
		• 0 — 'Unknown'							
		• 1 — 'Do Not Decrypt'							
		• 2 — 'Block'							
		• 3 — 'Block With Reset'							
		• 4 — 'Decrypt (Known Key)'							
		• 5 — 'Decrypt (Replace Key)'							
		• 6 — 'Decrypt (Resign)'							

Table B-43 Connection Statistics Data Block 6.0.x Fields (continued)

Field	Data Type	Description					
SSL Flow Status	uint16	Status of the SSL Flow. These values describe the reason					
		behind the action taken or the error message seen. Possible					
		values include:					
		• 23 — 'Internal Certificate List Unavailable'					
		• 24 — 'Internal Certificate Unavailable'					
		• 25 — 'Internal Certificate Fingerprint Unavailable'					
		• 26 — 'Server Certificate Validation Unavailable'					
		• 27 — 'Server Certificate Validation Failure'					
		• 28 — 'Invalid Action'					
SSL Flow Error	uint32	Detailed SSL error code. These values may be needed for support purposes.					

Table B-43 Connection Statistics Data Block 6.0.x Fields (continued)

Field	Data Type	Description
SSL Flow Messages	uint32	The messages exchanged between client and server during the SSL handshake. See http://tools.ietf.org/html/rfc5246 for more information.
		• 0x00000001 — NSE_MTHELLO_REQUEST
		• 0x00000002 — NSE_MTCLIENT_ALERT
		• 0x00000004 — NSE_MTSERVER_ALERT
		• 0x00000008 — NSE_MTCLIENT_HELLO
		• 0x00000010 — NSE_MTSERVER_HELLO
		• 0x00000020 — NSE_MTSERVER_CERTIFICATE
		• 0x00000040 — NSE_MTSERVER_KEY_EXCHANGE
		• 0x00000080 — NSE_MTCERTIFICATE_REQUEST
		• 0x00000100 — NSE_MTSERVER_HELLO_DONE
		• 0x00000200 — NSE_MTCLIENT_CERTIFICATE
		• 0x00000400 — NSE_MTCLIENT_KEY_EXCHANGE
		• 0x00000800 — NSE_MTCERTIFICATE_VERIFY
		• 0x00001000 —  NSE_MTCLIENT_CHANGE_CIPHER_SPEC
		• 0x00002000 — NSE_MTCLIENT_FINISHED
		• 0x00004000 —  NSE_MTSERVER_CHANGE_CIPHER_SPEC
		• 0x00008000 — NSE_MTSERVER_FINISHED
		• 0x00010000 — NSE_MTNEW_SESSION_TICKET
		• 0x00020000 — NSE_MTHANDSHAKE_OTHER
		• 0x00040000 — NSE_MTAPP_DATA_FROM_CLIENT
		• 0x00080000 — NSE_MTAPP_DATA_FROM_SERVER
SSL Flow Flags	uint64	The debugging level flags for an encrypted connection. Possible values include:
		0x00000001 — NSE_FLOWVALID - must be set for other fields to be valid
		0x00000002 — NSE_FLOWINITIALIZED - internal structures ready for processing
		0x00000004 — NSE_FLOWINTERCEPT - SSL session has been intercepted
String Block Type	uint32	Initiates a String data block containing the SSL Server Name. This
		value is always o.

Table B-43 Connection Statistics Data Block 6.0.x Fields (continued)

Field	Data Type	Description
String Block Length	uint32	The number of bytes included in the SSL Server Name String data block, including eight bytes for the block type and header fields plus the number of bytes in the SSL Server Name field.
SSL Server Name	string	Name provided in the server name indication in the SSL Client Hello.
SSL URL Category	uint32	Category of the flow as identified from the server name and certificate common name.
SSL Session ID	uint8[32]	Value of the session ID used during the SSL handshake when the client and server agree to do session reuse
SSL Session ID Length	uint8	Length of the SSL Session ID. While the session ID cannot exceed 32 bytes, it may be less than 32 bytes.
SSL Ticket ID	uint8[20]	Hash of the session ticket used when the client and server agree to use a session ticket.
SSL Ticket ID Length	uint8	Length of the SSL Ticket ID. While the ticket ID cannot exceed 20 bytes, it may be less than 20 bytes.
Network Analysis Policy revision	uint8[16]	Revision of the Network Analysis Policy associated with the connection event.
Endpoint Profile ID	uint32	ID number of the type of device used by the connection endpoint as identified by ISE. This is unique for each DC and resolved in metadata.
Security Group ID	uint32	ID number assigned to the user by ISE based on policy.
Location IPv6	uint8[16]	IP address of the interface communicating with ISE. Can be IPv4 or IPv6.
HTTP Response	uint32	Response code of the HTTP Request.
String Block Type	uint32	Initiates a String data block for the DNS query. 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 DNS query string.
DNS Query	string	The content of the query sent to the DNS server.
DNS Record Type	uint16	The numerical value for the type of DNS record.

Table B-43 Connection Statistics Data Block 6.0.x Fields (continued)

Field	Data Type	Description									
DNS Response	uint16	0 — NoError — No Error									
Type		1 — FormErr — Format Error									
		2 — ServFail — Server Failure									
		3 — NXDomain — Non-Existent Domain									
		4 — NotImp — Not Implemented									
		5 — Refused — Query Refused									
		6 — YXDomain — Name Exists when it should not									
		7 — YXRRSet — RR Set Exists when it should not									
		8 — NXRRSet — RR Set that should exist does not									
		9 — NotAuth — Not Authorized									
		10 — NotZone — Name not contained in zone									
		16 — BADSIG — TSIG Signature Failure  17 — BADKEY — Key not recognized  18 — BADTIME — Signature out of time window									
		_									
		17 — BADKEY — Key not recognized									
		19 — BADMODE — Bad TKEY Mode									
		20 — BADNAME — Duplicate key name									
		21 — BADALG — Algorithm not supported									
		22 — BADTRUNC — Bad Truncation									
		3841 — NXDOMAIN — NXDOMAIN response from firewall									
		3842 — SINKHOLE — Sinkhole response from firewall									
DNS TTL	uint32	The time to live for the DNS response, in seconds.									
Sinkhole UUID	uin8[16]	Revision UUID associated with this sinkhole object.									
Security Intelligence List 1	uint32	Security Intelligence List associated with the event. This maps to a Security Intelligence list in associated metadata. There may be two Security Intelligence lists associated with the connection.									
Security Intelligence List 2	uint32	Security Intelligence List associated with the event. This maps to a Security Intelligence list in associated metadata. There may be two Security Intelligence lists associated with the connection.									

## **Connection Statistics Data Block 6.1.x**

The connection statistics data block is used in connection data messages. Several new fields have been added to the Connection Statistics Data Block for 6.1.x. Fields have been added to support ISE Integration and Multiple Network Maps. The connection statistics data block for version 6.1+ has a block type of 163 in the series 1 group of blocks. It supersedes block type 160, Connection Statistics Data Block 6.0.x, page B-224. New fields have been added to support DNS lookup and Security Intelligence. It is superseded by block type 168, Connection Statistics Data Block 7.1+, page 4-118,

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 13 and an event code of 71. See Request Flags, page 2-13. 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 4-53.

The following diagram shows the format of a Connection Statistics data block for 6.1+:

Byte		1								2 3											
Bit	0 1 2	3 4	5	6 7	8	$9$ $\begin{bmatrix} 1\\0 \end{bmatrix}$	1	1 2	1 1 3 4	1 5	1 1 6 7	1 1	0 2	2	2 2 2 3	2 4	2 2 5	2 7	2 3	2 3	3
					Co	nnec	tion	Sta	itistic	s D	ata E	lock	Ту	pe (	163)						
					(	Conne	ectio	on S	Statist	tics	Data	Blo	ck I	Leng	gth						
	Device ID																				
									Ingr	ess	Zone	•									
	Ingress Zone, continued																				
	Ingress Zone, continued																				
	Ingress Zone, continued																				
	Egress Zone																				
	Egress Zone, continued																				
							I	Egr€	ess Zo	one	, con	inue	d								
							I	Egre	ess Zo	one	, con	inue	d								
								I	ngres	s Iı	nterfa	ice									
							Ing	gres	s Inte	rfa	ce, co	ontin	ued								
							Ing	gres	s Inte	rfa	ce, co	ontin	ued								
							Ing	gres	s Inte	rfa	ce, co	ontin	ued								
								I	Egres	s Ir	iterfa	ce									
							Eg	ress	s Inte	rfac	ce, co	ntin	ued								
							Eg	gress	s Inte	rfac	ce, co	ntin	ued								
							Eg	ress	s Inte	rfac	ce, co	ntin	ued								
								Ini	itiato	r IP	Add	ress									
						I	niti	ator	IP A	ddı	ress,	conti	nue	d							

Byte		0							1							2							3	3			
Bit	0 1	2	3 4	5	6 7	8	9	1 1 0 1	1 2	1 3	1	1 5	1 1 6 7	1 8	1 1 9	2 0		2 2	2 2 3	2 4	2 5	2 6	2 7	2 8	2 9	3	3
		Initiator IP Address, continued																									
		Initiator IP Address, continued																									
		Responder IP Address																									
		Responder IP Address, continued																									
		Responder IP Address, continued																									
		Responder IP Address, continued																									
								O	rigi	inal	Cl	ien	t IP	Ac	ddre	ess											
							Ori	igina	ıl C	Clien	t I	P A	ddre	ess	s, co	nti	nı	ued									
		Original Client IP Address, continued																									
		Original Client IP Address, continued																									
		Policy Revision																									
		Policy Revision, continued																									
													n, co														
								Po	olic	y Re			n, co	nt	tinu	ed											
										Т			ID	m													
					Dula	A at				Tur	ıne	115	Rule 1	ш —	,			D.	ıle I								
			I		Rule A			nt											tiat								
			- Г		espon														СР								
		Pr	otoco			dei	101						Νε	et F	Flov	v S	OI			1 10	15.	,					
						J		Ne	etFl	low	So	our	ce, co				•		5								
													ce, co														
	NetFlow Source, continued																										
	Ne		low loont.	Src	.,					Iı	ıst	and	e ID	)										ection nter			
	С	'x (	Ctr, c	ont	•							F	irst F	Pac	cke	t Ti	m	nest	amj	)							

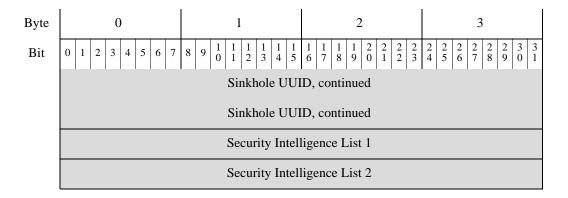
Byte	0	1 2 3								
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2								
	First Pkt Time, cont.	Last Packet Timestamp								
	Last Pkt Time, cont.	Initiator Transmitted Packets								
		Initiator Transmitted Packets, continued								
	Init. Tx Pkt, cont.	Responder Transmitted Packets								
		Responder Transmitted Packets, continued								
	Resp. Tx Pkt, cont.	Initiator Transmitted Bytes								
		Initiator Transmitted Bytes, continued								
	Init. Tx Bytes, cont.	Responder Transmitted Packets								
		Responder Transmitted Bytes, continued								
	Resp. Tx. Bytes, cont.	Initiator Packets Dropped								
	Initiator Packets Dropped, continued.									
	Init. Pkt. Drop, cont.	Responder Packets Dropped								
		Responder Packets Dropped, continued.								
	Resp. Pkt. Drop, cont.	Initiator Bytes Dropped								
		Initiator Bytes Dropped, continued.								
	Init. Byte Drop, cont.	Responder Bytes Dropped								
		Responder Bytes Dropped, continued.								
	Rsp. Byte Drop, cont.	QOS Applied Interface								
		QOS Applied Interface, continued								
		QOS Applied Interface, continued								
		QOS Applied Interface, continued								
	QOS Intf., cont.	QOS Rule ID								

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											
	QOS Rule ID, cont.	User ID											
	User ID, cont.	Application Protocol ID											
	App Prot. ID, cont.	URL Category											
	URL Category, cont.	URL Reputation											
	URL Rep., cont.	Rep., cont. Client Application ID											
	Client App ID, cont.												
	Web App. ID, cont.	Str. Block Type (0)											
Client URL	Str. Block Type, cont. String Block Length												
	Str. Block Len., cont.	Client App. URL											
S		String Block Type (0)											
NetBIOS Name		String Block Length											
ž	NetBIOS Name												
t sion		String Block Type (0)											
Client App Version		String Block Length											
Ap		Client Application Version											
		Monitor Rule 1											
		Monitor Rule 2											
		Monitor Rule 3											
		Monitor Rule 4											
		Monitor Rule 5											
	Monitor Rule 6												
		Monitor Rule 7											
	Soc Int Cra/Dat	Monitor Rule 8											
	Sec. Int. Src/Dst	Sec. Int. Layer File Event Count											

Byte		0								1						2						3																	
Bit	0	1	2	3	3 4	4 5	5	6	7	8		9	10	1 1		1 2	1			1 5	1			18	1 9	2 0	2		2 2 3	2	2	2 5	2 6	2 7	2	2 2	2	3	3
					Iı	ıtrı	ısi	on	I	Eve	nt	t C	o	unt	t												Ini	ti	atoı	·C	oı	ınt	ry						
						Re	sp	on	d	er (	Co	our	ıtı	ry							Original Client Country																		
							IC	OC	N	Jun	nt	er	•								Source Autonomous System																		
	S	Soi	urc	e	Αι	ıtoı	10	mo	οu	s S	у	ste	n	1, c	o	nti	n	ued	l				Ι	)e:	st	inat	ioı	n.	Aut	on	101	no	us	Sy	/S1	ten	1		
			De	est	tin	atic	n	Αı	ut	one	on	no	us	s S	ys	ste	m	1										,	SNN	ЛP	P I	n							
							5	SN	M	P (	Эı	ut											So	oui	rc	e T	OS	5			Ι	Des	tiı	nat	io	n T	О	S	
		S	ou	rc	e l	Ma	sk				D	es	ti	nat	ic	on ]	M	Iask	ζ.								Se	cı	ırity	C	Co	nte	xt						
																S	Se	ecur	rit	ty	C	ont	ex	ĸt															
																						it, c																	
																	ty	y Co	OI	nte	ex	t, c	or	nti	nı	ued													
				S	ecı	ırit	y	Co	n	tex	t,	со	n	tinı														1	/LA	N	[ ]]	<u> </u>							
Host																						Ty	_			)													
Referenced Host																						Le		_															
Refer																R	.e:	fere	en	ice	eed Host																		
ent															S	Stri	in	g B	310	oc.	ck Type (0)																		
User Agent																Stı	riı	ng l	B	lo	ock Length																		
Us																	1	Use	r	A	ge	ent.	••																
errer															S	Stri	in	g B	310	oc.	k	Ty	pe	e ((	0)	)													
HTTP Referrer																Stı	riı	ng l	B	lo	ck	c Le	n	gtl	h														
HTT																ŀ	ď	ГТІ	P	Re	ef	erre	er.	•••															
		SSL Certif							ïc	cat	te	Fin	ıg	erj	pı	int																							
		SSL Certificate							F	ingerprint, continued																													
											5	SS	L	Ce	ert	tifi	ca	ate !	F	ingerprint, continued																			
											5	SS	L	Ce	ert	tifi	ca	ate !	F	inį	ge	erpr	in	ıt,	C	onti	nu	e	d										
		SSL Certificate							F	inį	ge	erpr	in	ıt,	C	onti	nu	e	d																				

Byte	0				0 1					2				3									
Bit	0 1 2	3 4	4 5	6	7 8	9	1 1 0 1		1 1 3 4	1 5	1 1 6 7	1 8	1 2	2 2	2 2	2 3	2 4	2 2 5 6	2 7	2 2	$\begin{bmatrix} 3 \\ 0 \end{bmatrix}$	3	
									SSL	Po	licy l	D											
							S	SSL	Polic	y I	D, co	ntiı	nued										
		SSL Pol								уΙ	y ID, continued												
							S	SSL	Polic	y I	ID, continued												
						SSL Rule ID																	
			SS	L Ci		her Suite SSL Version									SSL Srv Cert. Stat.  SSL Actual Action								
							SL Srv Cert. Stat., cont.											SL A	ctu	al A	ction	n	
		SSL Actual Action, cont.						SS	L Ex	pec	ted A	cti	on				SSL Flow Status						
	SSL Flow Status, cont. SSL Flow Error									•													
	SSL F	Flow ntinu	ror, SSL Flow Messages																				
	SS Me cor							S	SL 1	Flow	Fla	ags	}										
							SSL Flow Flags, continued																
ames	SSL F	low ntinu	w Flags, nued String Block Type (0)										(0)										
Server Names	String 1 (0), o										Stri	ng I	Blocl	ιLe	eng	gth							
SSF	Strii Length	ng B	locl ntin	c ued							SSI	. Se	erver	Na	me	·							
								S	SL U	RL	Cate	gor	У										
									SSL	Ses	sion	ID											
							S	SL S	Sessi	on l	D, co	onti	nuec										
							S	SL S	Sessi	on l	D, co	onti	nuec										
		SSL Session							on l	n ID, continued													
							S	SL S	Sessi	on l	D, co	onti	nuec										
								SL S	Sessi	on l	D, co	onti	nuec										

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										
		SSL Session I	ID, continued											
		SSL Session 1	D, continued											
	SSL Session ID Length		SSL Ticket ID											
		SSL Ticket I	ID, continued											
		SSL Ticket II	ID, continued											
		SSL Ticket I	ID, continued											
		SSL Ticket II	ID, continued											
	SSL Ticket ID, cont.	SSL Ticket ID Length	Network Analysis Policy Revision											
	]	Network Analysis Polic	icy Revision, continued											
	]	Network Analysis Polic	cy Revision, continued	d										
	1	Network Analysis Polic	cy Revision, continued	d										
	Network Analysis conti		Endpoint Profile ID											
	Endpoint Profile	e ID, continued	Security Group ID											
	Security Group	ID, continued	Location IPv6											
		Location IPv	76, continued											
		Location IPv	6, continued											
		Location IPv	6, continued											
	Location IPv	6, continued	HTTP F	Response										
ıery	HTTP Respon		String Blo	ck Type (0)										
DNS Query	String Block Typ		String Block Length											
[Q	String Block Le		DNS Query											
	DNS Rec		DNS Response Type											
		DNS												
		Sinkhole UUI												



The following table describes the fields of the Connection Statistics data block for 6.1.x.

Table B-44 Connection Statistics Data Block 6.1+ Fields

Field	Data Type	Description
Connection Statistics Data Block Type	uint32	Initiates a Connection Statistics data block for 6.1.x. The value is always 163.
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.
Original Client IP Address	uint8[16]	IP address of the host behind the proxy that originated the request, 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.
Tunnel Rule ID	uint32	Internal identifier for the tunnel 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).

Table B-44 Connection Statistics Data Block 6.1+ Fields (continued)

Field	Data Type	Description
Rule Reason	uint32	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.
Initiator Packets Dropped	uint64	Number of packets dropped from the session initiator due to rate limiting.
Responder Packets Dropped	uint64	Number of packets dropped from the session responder due to rate limiting.
Initiator Bytes Dropped	uint64	Number of bytes dropped from the session initiator due to rate limiting.
Responder Bytes Dropped	uint64	Number of bytes dropped from the session responders due to rate limiting.
QOS Applied Interface	uint8[16]	For rate-limited connections, the name of the interface on which rate limiting is applied.
QOS Rule ID	uint32	Internal ID number of the Quality of Service rule applied to the connection, if applicable.
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.

Table B-44 Connection Statistics Data Block 6.1+ Fields (continued)

Field	Data Type	Description
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.
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.

Table B-44 Connection Statistics Data Block 6.1+ Fields (continued)

Field	Data Type	Description
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 block list.
Security Intelligence Layer	uint8	The IP layer that matched the IP block list.
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.
Original Client Country	uint 16	Code for the country of the host behind the proxy which originated the request.
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.
VLAN ID	uint16	VLAN identification number that indicates which VLAN the host is a member of.
String Block Type	uint32	Initiates a String data block containing the Referenced Host. This value is always 0.
String Block Length	uint32	The number of bytes included in the Referenced Host String data block, including eight bytes for the block type and header fields plus the number of bytes in the Referenced Host field.
Referenced Host	string	Host name information provided in HTTP or DNS.

Table B-44 Connection Statistics Data Block 6.1+ Fields (continued)

Field	Data Type	Description
String Block Type	uint32	Initiates a String data block containing the User Agent. This value is always 0.
String Block Length	uint32	The number of bytes included in the User Agent String data block, including eight bytes for the block type and header fields plus the number of bytes in the User Agent field.
User Agent	string	Information from the UserAgent header field in the session.
String Block Type	uint32	Initiates a String data block containing the HTTP Referrer. This value is always 0.
String Block Length	uint32	The number of bytes included in the HTTP Referrer String data block, including eight bytes for the block type and header fields plus the number of bytes in the HTTP Referrer field.
HTTP Referrer	string	The site from which a page originated. This is found int he Referred header information in HTTP traffic.
SSL Certificate Fingerprint	uint8[20]	SHA1 hash of the SSL Server certificate.
SSL Policy ID	uint8[16]	ID number of the SSL policy that handled the connection.
SSL Rule ID	uint32	ID number of the SSL rule or default action that handled the connection.
SSL Cipher Suite	uint16	Encryption suite used by the SSL connection. The value is stored in decimal format. See  www.iana.org/assignments/tls-parameters/tls-parameters.
SSL Version	uint8	xhtml for the cipher suite designated by the value.
SSL Version SSL Server	uint32	The SSL or TLS protocol version used to encrypt the connection.  The status of the SSL certificate. Possible values include:
Certificate Status	umt32	O — Not checked — The server certificate status was not evaluated.
		• 1 — Unknown — The server certificate status could not be determined.
		• 2 — Valid — The server certificate is valid.
		• 4 — Self-signed — The server certificate is self-signed.
		• 16 — Invalid Issuer — The server certificate has an invalid issuer.
		• 32 — Invalid Signature — The server certificate has an invalid signature.
		• 64 — Expired — The server certificate is expired.
		• 128 — Not valid yet — The server certificate is not yet valid.
		• 256 — Revoked — The server certificate has been revoked.

Table B-44 Connection Statistics Data Block 6.1+ Fields (continued)

Field	Data Type	Description
SSL Actual Action	uint16	The action performed on the connection based on the SSL Rule.  This may differ from the expected action, as the action as specified in the rule may be impossible. Possible values include:
		• 0 — 'Unknown'
		• 1 — 'Do Not Decrypt'
		• 2 — 'Block'
		• 3 — 'Block With Reset'
		• 4 — 'Decrypt (Known Key)'
		• 5 — 'Decrypt (Replace Key)'
		• 6 — 'Decrypt (Resign)'
SSL Expected Action	uint16	The action which should be performed on the connection based on the SSL Rule. Possible values include:
		• 0 — 'Unknown'
		• 1 — 'Do Not Decrypt'
		• 2 — 'Block'
		• 3 — 'Block With Reset'
		• 4 — 'Decrypt (Known Key)'
		• 5 — 'Decrypt (Replace Key)'
		• 6 — 'Decrypt (Resign)'

Table B-44 Connection Statistics Data Block 6.1+ Fields (continued)

Field	Data Type	Description
SSL Flow Status	uint16	Status of the SSL Flow. These values describe the reason
		behind the action taken or the error message seen. Possible
		values include:
		• 0 — 'Unknown'
		• 1 — 'No Match'
		• 2 — 'Success'
		• 3 — 'Uncached Session'
		• 4 — 'Unknown Cipher Suite'
		• 5 — 'Unsupported Cipher Suite'
		• 6 — 'Unsupported SSL Version'
		• 7 — 'SSL Compression Used'
		8 — 'Session Undecryptable in Passive Mode'
		• 9 — 'Handshake Error'
		• 10 — 'Decryption Error'
		• 11 — 'Pending Server Name Category Lookup'
		• 12 — 'Pending Common Name Category Lookup'
		• 13 — 'Internal Error'
		• 14 — 'Network Parameters Unavailable'
		• 15 — 'Invalid Server Certificate Handle'
		• 16 — 'Server Certificate Fingerprint Unavailable'
		• 17 — 'Cannot Cache Subject DN'
		• 18 — 'Cannot Cache Issuer DN'
		• 19 — 'Unknown SSL Version'
		• 20 — 'External Certificate List Unavailable'
		• 21 — 'External Certificate Fingerprint Unavailable'
		• 22 — 'Internal Certificate List Invalid'
		• 23 — 'Internal Certificate List Unavailable'
		• 24 — 'Internal Certificate Unavailable'
		15 — 'Internal Certificate Fingerprint Unavailable'
		26 — 'Server Certificate Validation Unavailable'
		'Server Certificate Validation Failure'
		• 28 — 'Invalid Action'
SSL Flow Error	uint32	Detailed SSL error code. These values may be needed for support purposes.

Table B-44 Connection Statistics Data Block 6.1+ Fields (continued)

Field	Data Type	Description
SSL Flow Messages	uint32	The messages exchanged between client and server during the SSL handshake. See http://tools.ietf.org/html/rfc5246 for more information.
		• 0x00000001 — NSE_MTHELLO_REQUEST
		• 0x00000002 — NSE_MTCLIENT_ALERT
		• 0x00000004 — NSE_MTSERVER_ALERT
		0x00000008 — NSE_MTCLIENT_HELLO
		• 0x00000010 — NSE_MTSERVER_HELLO
		• 0x00000020 — NSE_MTSERVER_CERTIFICATE
		• 0x00000040 — NSE_MTSERVER_KEY_EXCHANGE
		0x00000080 — NSE_MTCERTIFICATE_REQUEST
		• 0x00000100 — NSE_MTSERVER_HELLO_DONE
		• 0x00000200 — NSE_MTCLIENT_CERTIFICATE
		• 0x00000400 — NSE_MTCLIENT_KEY_EXCHANGE
		• 0x00000800 — NSE_MTCERTIFICATE_VERIFY
		0x00001000 —     NSE_MTCLIENT_CHANGE_CIPHER_SPEC
		0x00002000 — NSE_MTCLIENT_FINISHED
		0x00004000 —     NSE_MTSERVER_CHANGE_CIPHER_SPEC
		• 0x00008000 — NSE_MTSERVER_FINISHED
		• 0x00010000 — NSE_MTNEW_SESSION_TICKET
		• 0x00020000 — NSE_MTHANDSHAKE_OTHER
		• 0x00040000 — NSE_MTAPP_DATA_FROM_CLIENT
		• 0x00080000 — NSE_MTAPP_DATA_FROM_SERVER
SSL Flow Flags	uint64	The debugging level flags for an encrypted connection. Possible values include:
		0x00000001 — NSE_FLOWVALID - must be set for other fields to be valid
		0x00000002 — NSE_FLOWINITIALIZED - internal structures ready for processing
		0x00000004 — NSE_FLOWINTERCEPT - SSL session has been intercepted
String Block Type	uint32	Initiates a String data block containing the SSL Server Name. This value is always 0.

Table B-44 Connection Statistics Data Block 6.1+ Fields (continued)

Field	Data Type	Description	
String Block Length	uint32	The number of bytes included in the SSL Server Name String data block, including eight bytes for the block type and header fields plus the number of bytes in the SSL Server Name field.	
SSL Server Name	string	Name provided in the server name indication in the SSL Client Hello.	
SSL URL Category	uint32	Category of the flow as identified from the server name and certificate common name.	
SSL Session ID	uint8[32]	Value of the session ID used during the SSL handshake when the client and server agree to do session reuse	
SSL Session ID Length	uint8	Length of the SSL Session ID. While the session ID cannot exceed 32 bytes, it may be less than 32 bytes.	
SSL Ticket ID	uint8[20]	Hash of the session ticket used when the client and server agree to use a session ticket.	
SSL Ticket ID Length	uint8	Length of the SSL Ticket ID. While the ticket ID cannot exceed 20 bytes, it may be less than 20 bytes.	
Network Analysis Policy revision	uint8[16]	Revision of the Network Analysis Policy associated with the connection event.	
Endpoint Profile ID	uint32	ID number of the type of device used by the connection endpoint as identified by ISE. This is unique for each DC and resolved in metadata.	
Security Group ID	uint32	ID number assigned to the user by ISE based on policy.	
Location IPv6	uint8[16]	IP address of the interface communicating with ISE. Can be IPv4 or IPv6.	
HTTP Response	uint32	Response code of the HTTP Request.	
String Block Type	uint32	Initiates a String data block for the DNS query. 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 DNS query string.	
DNS Query	string	The content of the query sent to the DNS server.	
DNS Record Type	uint16	The numerical value for the type of DNS record.	
DNS Response Type	uint16	The numerical value for the type of DNS response.	
DNS TTL	uint32	The time to live for the DNS response, in seconds.	
Sinkhole UUID	uin8[16]	Revision UUID associated with this sinkhole object.	
Security Intelligence List 1	uint32	Security Intelligence List associated with the event. This maps to a Security Intelligence list in associated metadata. There may be two Security Intelligence lists associated with the connection.	
Security Intelligence List 2	uint32	Security Intelligence List associated with the event. This maps to a Security Intelligence list in associated metadata. There may be two Security Intelligence lists associated with the connection.	

## **Connection Statistics Data Block 6.2-6.7.x**

The connection statistics data block is used in connection data messages. A third Security Intelligence field has been added to Connection Statistics Data Block for 6.2-6.7.x. The connection statistics data block for version 6.2-6.7.x has a block type of 168 in the series 1 group of blocks. It supersedes block type 163, Connection Statistics Data Block 6.1.x, page B-239. It is superseded by block type 173.

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 15 and an event code of 71. See Request Flags, page 2-13. 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 4-53.

The following diagram shows the format of a Connection Statistics data block for 6.2-6.7.x:

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	
		Connection Statistics Data Block Type (168)			
	Connection Statistics Data Block Length				
		Devid	ce ID		
		Ingress	s 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 Interfa	ace, continued		
		Ingress Interface, continued			
	Ingress Interface, continued				
		Egress Interface			
		Egress Interfa	ce, continued		
		Egress Interfa	ce, 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	2 2 2 2 2 2 3 3 3 4 5 6 7 8 9 0 1
	Egress Interface, continued			
		Initiator IP Address		
		Initiator IP Add	ress, continued	
		Initiator IP Add	ress, continued	
		Initiator IP Add	ress, continued	
		Responder	IP Address	
		Responder IP Ad	dress, continued	
		Responder IP Ad	dress, continued	
		Responder IP Ad	dress, continued	
		Original Clien	nt IP Address	
		Original Client IP	Address, continued	
	Original Client IP Address, continued			
	Original Client IP Address, continued			
	Policy Revision			
	Policy Revision, continued			
	Policy Revision, continued			
	Policy Revision, continued			
		Rule		
	2.1	Tunnel 1		<b>D</b>
	Rule A			Reason
	Rule Reas			ator Port
	Respond	ler Port		P Flags
	Protocol	NotElou Cour	NetFlow Source	
		NetFlow Sour		
		NetFlow Sour		
		NetFlow Sour	ce, conunuea	

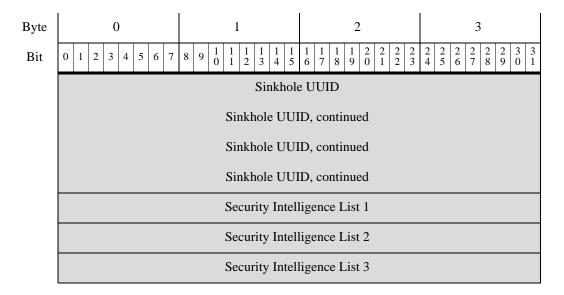
Byte	0	1	2		3
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 6 7 8 9 0 1 2	2 2 2 2 3 4 5 6	2 2 2 3 3 7 8 9 0 1
	NetFlow Src., cont.	Instan	ice ID		nnection
	Cx Ctr, cont.	I	First Packet Timest	amp	
	First Pkt Time, cont.	1	Last Packet Timest	ımp	
	Last Pkt Time, cont.	Init	tiator Transmitted I	ackets	
		Initiator Transmitted	d Packets, continue	1	
	Init. Tx Pkt, cont.	Resp	onder Transmitted	Packets	
		Responder Transmitte	ed Packets, continu	ed	
	Resp. Tx Pkt, cont.	In	itiator Transmitted	Bytes	
		Initiator Transmitte	ed Bytes, continued		
	Init. Tx Bytes, cont.	Resp	oonder Transmitted	Packets	
		Responder Transmit	ted Bytes, continue	d	
	Resp. Tx. Bytes, cont.	Ir	nitiator Packets Dro	pped	
		Initiator Packets D	ropped, continued.		
	Init. Pkt. Drop, cont.	Re	sponder Packets Di	opped	
		Responder Packets l	Dropped, continued		
	Resp. Pkt. Drop, cont.	]	Initiator Bytes Drop	ped	
		Initiator Bytes Dr	opped, continued.		
	Init. Byte Drop, cont.	R	esponder Bytes Dro	pped	
		Responder Bytes D	Propped, continued.		
	Rsp. Byte Drop, cont.	•	QOS Applied Inter	ace	
		QOS Applied Int	erface, continued		
		QOS Applied Int	erface, continued		

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 2 3 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1	
		QOS Applied Interface, continued	
	QOS Intf., cont.	QOS Rule ID	
	QOS Rule ID, cont.	User ID	
	User ID, cont.	Application Protocol ID	
	App Prot. ID, cont.	URL Category	
	URL Category, cont.	URL Reputation	
	URL Rep., cont.	Client Application ID	
	Client App ID, cont.	Web Application ID	
	Web App. ID, cont.	Str. Block Type (0)	
Client URL	Str. Block Type, cont.	String Block Length	
_	Str. Block Len., cont.	Client App. URL	
S		String Block Type (0)	
NetBIOS Name		String Block Length	
Ž		NetBIOS Name	
ion		String Block Type (0)	
Client App Version		String Block Length	
Apl		Client Application Version	
		Monitor Rule 1	
	Monitor Rule 2		
	Monitor Rule 3		
	Monitor Rule 4		
		Monitor Rule 5	
		Monitor Rule 6	
	Monitor Rule 7		

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 2 2 2 2 2 3 3 3 4 5 6 7 8 9 0 1			
Monitor Rule 8	Monitor Rule 8			
Sec. Int. Src/Dst Sec. Int. Layer File Ev	ent Count			
Intrusion Event Count Initiato	Country			
Responder Country Original C	ient Country			
IOC Number Source Autor	nomous System			
Source Autonomous System, continued Destination Au	onomous System			
Destination Autonomous System SN	MP In			
SNMP Out Source TOS	Destination TOS			
	y Context			
Security Context				
Security Context, continued				
Security Context, continued				
,	Security Context, continued VLAN ID			
9Н	String Block Type (0)			
String Block Length  Referenced Host				
e e e e e e e e e e e e e e e e e e e				
String Block Type (0)				
String Block Type (6)  String Block Length  User Agent				
User Agent	User Agent			
String Block Type (0)				
String Block Type (0)  String Block Length  HTTP Referrer				
HTTP Referrer				
SSL Certificate Fingerprint				
SSL Certificate Fingerprint, continued				
SSL Certificate Fingerprint, 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		
	SSL Certificate Fingerprint, continued					
	SSL Certificate Fingerprint, continued					
		SSL Policy ID				
		SSL Policy I	D, continued			
		SSL Policy I	D, continued			
		SSL Policy I	D, continued			
		SSL R	ule ID			
	SSL Cipl	ner Suite	SSL Version	SSL Srv Cert. Stat.		
	S	SL Srv Cert. Stat., con	t.	SSL Actual Action		
	SSL Actual Action, cont.	SSL Expec	eted Action	SSL Flow Status		
	SSL Flow Status, cont.	SSL Flow Error				
	SSL Flow Error, continued SSL Flow Messages					
	SSL Flow Messages, continued	Messages,				
		SSL Flow Fla	gs, continued			
ames	SSL Flow Flags, continued		String Block Type (0)			
SSL Server N	String Block Type (0), continued		String Block Length			
SSF 8	String Block Length, continued		SSL Server Name			
		SSL URL	Category			
		SSL Ses	ssion ID			
	SSL Session ID, continued					
		SSL Session	ID, continued			
		SSL Session	ID, 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     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		
	SSL Session ID, continued					
		SSL Session ID, continued				
		SSL Session ID, continued				
		SSL Session ID, continued				
	SSL Session ID Length		SSL Ticket ID			
		SSL Ticket I	D, continued			
		SSL Ticket I	D, continued			
		SSL Ticket I	D, continued			
		SSL Ticket I	D, continued			
	SSL Ticket ID, cont.	SSL Ticket ID Length	Network Analysis	Policy Revision		
	]	Network Analysis Police	cy Revision, continued			
	Network Analysis Policy Revision, continued					
	Network Analysis Policy Revision, continued					
	Network Analysis Policy Revision, Endpoint Profile ID continued			rofile ID		
	Endpoint Profil	e ID, continued	Security G	Security Group ID		
	Security Group	DID, continued	Location IPv6			
		Location IPv	6, continued			
		Location IPv	6, continued			
		Location IPv	6, continued			
	Location IPv	6, continued	HTTP Re	esponse		
ery	HTTP Respor	ise, continued	String Block	Type (0)		
DNS Query	String Block Typ	pe (0), continued	String Block Length			
D	String Block Le	ength, continued	DNS Query			
	DNS Rec	ord Type	DNS Respon	nse Type		
		DNS	TTL			



The following table describes the fields of the Connection Statistics data block for 6.2-6.7.x.

Table B-45 Connection Statistics Data Block 6.2-6.7.x Fields

Field	Data Type	Description
Connection Statistics Data Block Type	uint32	Initiates a Connection Statistics data block for 6.2-6.7.x. The value is always 168.
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.
Original Client IP Address	uint8[16]	IP address of the host behind the proxy that originated the request, 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.

Table B-45 Connection Statistics Data Block 6.2-6.7.x Fields (continued)

Field	Data Type	Description	
Tunnel Rule ID	uint32	Internal identifier for the tunnel 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	uint32	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.	
Initiator Packets Dropped	uint64	Number of packets dropped from the session initiator due to rate limiting.	
Responder Packets Dropped	uint64	Number of packets dropped from the session responder due to rate limiting.	
Initiator Bytes Dropped	uint64	Number of bytes dropped from the session initiator due to rate limiting.	
Responder Bytes Dropped	uint64	Number of bytes dropped from the session responders due to rate limiting.	
QOS Applied Interface	uint8[16]	For rate-limited connections, the name of the interface on which rate limiting is applied.	
QOS Rule ID	uint32	Internal ID number of the Quality of Service rule applied to the connection, if applicable.	

Table B-45 Connection Statistics Data Block 6.2-6.7.x 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-45 Connection Statistics Data Block 6.2-6.7.x 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 block list.
Security Intelligence Layer	uint8	The IP layer that matched the IP block list.
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.
Original Client Country	uint 16	Code for the country of the host behind the proxy which originated the request.
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.
VLAN ID	uint16	VLAN identification number that indicates which VLAN the host is a member of.
String Block Type	uint32	Initiates a String data block containing the Referenced Host. This value is always 0.

Table B-45 Connection Statistics Data Block 6.2-6.7.x Fields (continued)

Field	Data Type	Description
String Block Length	uint32	The number of bytes included in the Referenced Host String data block, including eight bytes for the block type and header fields plus the number of bytes in the Referenced Host field.
Referenced Host	string	Host name information provided in HTTP or DNS.
String Block Type	uint32	Initiates a String data block containing the User Agent. This value is always 0.
String Block Length	uint32	The number of bytes included in the User Agent String data block, including eight bytes for the block type and header fields plus the number of bytes in the User Agent field.
User Agent	string	Information from the UserAgent header field in the session.
String Block Type	uint32	Initiates a String data block containing the HTTP Referrer. This value is always 0.
String Block Length	uint32	The number of bytes included in the HTTP Referrer String data block, including eight bytes for the block type and header fields plus the number of bytes in the HTTP Referrer field.
HTTP Referrer	string	The site from which a page originated. This is found int he Referred header information in HTTP traffic.
SSL Certificate Fingerprint	uint8[20]	SHA1 hash of the SSL Server certificate.
SSL Policy ID	uint8[16]	ID number of the SSL policy that handled the connection.
SSL Rule ID	uint32	ID number of the SSL rule or default action that handled the connection.
SSL Cipher Suite	uint16	Encryption suite used by the SSL connection. The value is stored in decimal format. See  www.iana.org/assignments/tls-parameters/tls-parameters.  xhtml for the cipher suite designated by the value.
SSL Version	uint8	The SSL or TLS protocol version used to encrypt the connection.
SSL Server	uint32	The status of the SSL certificate. Possible values include:
Certificate Status		• 0 — Not checked — The server certificate status was not evaluated.
		• 1 — Unknown — The server certificate status could not be determined.
		• 2 — Valid — The server certificate is valid.
		• 4 — Self-signed — The server certificate is self-signed.
		• 16 — Invalid Issuer — The server certificate has an invalid issuer.
		• 32 — Invalid Signature — The server certificate has an invalid signature.
		• 64 — Expired — The server certificate is expired.
		• 128 — Not valid yet — The server certificate is not yet valid.
		• 256 — Revoked — The server certificate has been revoked.

Table B-45 Connection Statistics Data Block 6.2-6.7.x Fields (continued)

Field	Data Type	Description
SSL Actual Action	uint16	The action performed on the connection based on the SSL Rule. This may differ from the expected action, as the action as specified in the rule may be impossible. Possible values include:
		• 0 — 'Unknown'
		• 1 — 'Do Not Decrypt'
		• 2 — 'Block'
		• 3 — 'Block With Reset'
		• 4 — 'Decrypt (Known Key)'
		• 5 — 'Decrypt (Replace Key)'
		• 6 — 'Decrypt (Resign)'
SSL Expected Action	uint16	The action which should be performed on the connection based on the SSL Rule. Possible values include:
		• 0 — 'Unknown'
		• 1 — 'Do Not Decrypt'
		• 2 — 'Block'
		• 3 — 'Block With Reset'
		• 4 — 'Decrypt (Known Key)'
		• 5 — 'Decrypt (Replace Key)'
		• 6 — 'Decrypt (Resign)'

Table B-45 Connection Statistics Data Block 6.2-6.7.x Fields (continued)

Field	Data Type	Description
SSL Flow Status	uint16	Status of the SSL Flow. These values describe the reason
		behind the action taken or the error message seen. Possible
		values include:
		<ul> <li>0 — 'Unknown'</li> <li>1 — 'No Match'</li> <li>2 — 'Success'</li> <li>3 — 'Uncached Session'</li> <li>4 — 'Unknown Cipher Suite'</li> <li>5 — 'Unsupported Cipher Suite'</li> <li>6 — 'Unsupported SSL Version'</li> <li>7 — 'SSL Compression Used'</li> <li>8 — 'Session Undecryptable in Passive Mode'</li> <li>9 — 'Handshake Error'</li> </ul>
		<ul> <li>10 — 'Decryption Error'</li> <li>11 — 'Pending Server Name Category Lookup'</li> <li>12 — 'Pending Common Name Category Lookup'</li> </ul>
		<ul> <li>13 — 'Internal Error'</li> <li>14 — 'Network Parameters Unavailable'</li> <li>15 — 'Invalid Server Certificate Handle'</li> </ul>
		<ul> <li>16 — 'Server Certificate Fingerprint Unavailable'</li> <li>17 — 'Cannot Cache Subject DN'</li> <li>18 — 'Cannot Cache Issuer DN'</li> </ul>
		<ul> <li>19 — 'Unknown SSL Version'</li> <li>20 — 'External Certificate List Unavailable'</li> </ul>
		<ul> <li>21 — 'External Certificate Fingerprint Unavailable'</li> <li>22 — 'Internal Certificate List Invalid'</li> <li>23 — 'Internal Certificate List Unavailable'</li> </ul>
		<ul> <li>24 — 'Internal Certificate Unavailable'</li> <li>25 — 'Internal Certificate Fingerprint Unavailable'</li> <li>26 — 'Server Certificate Validation Unavailable'</li> </ul>
		<ul> <li>27 — 'Server Certificate Validation Failure'</li> <li>28 — 'Invalid Action'</li> </ul>
SSL Flow Error	uint32	Detailed SSL error code. These values may be needed for support purposes.

Table B-45 Connection Statistics Data Block 6.2-6.7.x Fields (continued)

Field	Data Type	Description
SSL Flow Messages	uint32	The messages exchanged between client and server during the SSL handshake. See http://tools.ietf.org/html/rfc5246 for more information.
		• 0x00000001 — NSE_MTHELLO_REQUEST
		• 0x00000002 — NSE_MTCLIENT_ALERT
		• 0x00000004 — NSE_MTSERVER_ALERT
		• 0x00000008 — NSE_MTCLIENT_HELLO
		• 0x00000010 — NSE_MTSERVER_HELLO
		• 0x00000020 — NSE_MTSERVER_CERTIFICATE
		• 0x00000040 — NSE_MTSERVER_KEY_EXCHANGE
		• 0x00000080 — NSE_MTCERTIFICATE_REQUEST
		• 0x00000100 — NSE_MTSERVER_HELLO_DONE
		• 0x00000200 — NSE_MTCLIENT_CERTIFICATE
		• 0x00000400 — NSE_MTCLIENT_KEY_EXCHANGE
		• 0x00000800 — NSE_MTCERTIFICATE_VERIFY
		• 0x00001000 —  NSE_MTCLIENT_CHANGE_CIPHER_SPEC
		• 0x00002000 — NSE_MTCLIENT_FINISHED
		• 0x00004000 —  NSE_MTSERVER_CHANGE_CIPHER_SPEC
		• 0x00008000 — NSE_MTSERVER_FINISHED
		• 0x00010000 — NSE_MTNEW_SESSION_TICKET
		• 0x00020000 — NSE_MTHANDSHAKE_OTHER
		• 0x00040000 — NSE_MTAPP_DATA_FROM_CLIENT
		• 0x00080000 — NSE_MTAPP_DATA_FROM_SERVER
SSL Flow Flags	uint64	The debugging level flags for an encrypted connection. Possible values include:
		0x00000001 — NSE_FLOWVALID - must be set for other fields to be valid
		0x00000002 — NSE_FLOWINITIALIZED - internal structures ready for processing
		0x00000004 — NSE_FLOWINTERCEPT - SSL session has been intercepted
String Block Type	uint32	Initiates a String data block containing the SSL Server Name. This value is always 0.

Table B-45 Connection Statistics Data Block 6.2-6.7.x Fields (continued)

Field	Data Type	Description
String Block Length	uint32	The number of bytes included in the SSL Server Name String data block, including eight bytes for the block type and header fields plus the number of bytes in the SSL Server Name field.
SSL Server Name	string	Name provided in the server name indication in the SSL Client Hello.
SSL URL Category	uint32	Category of the flow as identified from the server name and certificate common name.
SSL Session ID	uint8[32]	Value of the session ID used during the SSL handshake when the client and server agree to do session reuse
SSL Session ID Length	uint8	Length of the SSL Session ID. While the session ID cannot exceed 32 bytes, it may be less than 32 bytes.
SSL Ticket ID	uint8[20]	Hash of the session ticket used when the client and server agree to use a session ticket.
SSL Ticket ID Length	uint8	Length of the SSL Ticket ID. While the ticket ID cannot exceed 20 bytes, it may be less than 20 bytes.
Network Analysis Policy revision	uint8[16]	Revision of the Network Analysis Policy associated with the connection event.
Endpoint Profile ID	uint32	ID number of the type of device used by the connection endpoint as identified by ISE. This is unique for each DC and resolved in metadata.
Security Group ID	uint32	ID number assigned to the user by ISE based on policy.
Location IPv6	uint8[16]	IP address of the interface communicating with ISE. Can be IPv4 or IPv6.
HTTP Response	uint32	Response code of the HTTP Request.
String Block Type	uint32	Initiates a String data block for the DNS query. 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 DNS query string.
DNS Query	string	The content of the query sent to the DNS server.
DNS Record Type	uint16	The numerical value for the type of DNS record.
DNS Response Type	uint16	The numerical value for the type of DNS response.
DNS TTL	uint32	The time to live for the DNS response, in seconds.
Sinkhole UUID	uin8[16]	Revision UUID associated with this sinkhole object.
Security Intelligence List 1	uint32	Security Intelligence List associated with the event. This maps to a Security Intelligence list in associated metadata. There may be three Security Intelligence lists associated with the connection.

Table B-45 Connection Statistics Data Block 6.2-6.7.x Fields (continued)

Field	Data Type	Description
Security Intelligence List 2	uint32	Security Intelligence List associated with the event. This maps to a Security Intelligence list in associated metadata. There may be three Security Intelligence lists associated with the connection.
Security Intelligence List 3	uint32	Security Intelligence List associated with the event. This maps to a Security Intelligence list in associated metadata. There may be three Security Intelligence lists associated with the connection.

## **Connection Statistics Data Block 7.0**

The connection statistics data block is used in connection data messages. Security Group Tag, virtual routing and forwarding, and dynamic attribute fields have been added to Connection Statistics Data Block for 7.0+. The connection statistics data block for version 7.0+ has a block type of 173 in the series 1 group of blocks. It supersedes block type 168, Connection Statistics Data Block 6.2-6.7.x, page B-256. It is superseded by block type 174

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 16 and an event code of 71. See Request Flags, page 2-13. 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 4-53.

The following diagram shows the format of a Connection Statistics data block for 7.0:

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										
		Connection Statistics I	Data Block Type (173)	)										
	Connection Statistics Data Block Length													
		Devic	ce ID											
		Ingress	s Zone											
		Ingress Zone	e, continued											
		Ingress Zone	e, continued											
		Ingress Zone	1											
	Egress Zone													
		Egress Zone	e, continued											
		Egress Zone	e, continued											
		Egress Zone	e, continued											

7

Byte		0					1	1			2							3						
Bit	0 1 2	3 4	8		1 1 0 1	1 1 2 3	1 4	1 5	1 1 6 7	1 1 8	2 0	2 2 1 2	2 3	2 4	2 2 6	2 7	2 8	2 3	3 1					
								In	gres	s I	nterfa	ice												
							Ing	gress	Inte	rfa	ice, co	ontin	ued											
							Ing	gress	Inte	rfa	ice, co	ontin	ued											
							Ing	gress	Inte	rfa	ice, co	ontin	ued											
								E	gres	s I	nterfa	ce												
	Egress Interface, continued  Egress Interface, continued  Egress Interface, continued																							
	Initiator IP Address																							
							Initi	ator I	PΑ	dd	ress,	conti	nue	d										
							Initi	ator I	PΑ	dd	ress,	conti	nue	d										
							Initi	ator I	PA	dd	ress,	conti	nue	d										
								Resp	ond	er	IP Ac	dres	S											
						F	Respo	onder	IP.	Ad	dress	, con	tinu	ed										
						F	Respo	onder	IP.	Ad	dress	, con	tinu	ed										
						F	Respo	onder	IP.	Ad	dress	, con	tinu	ed										
							O	rigina	ıl Cl	liei	nt IP	Addr	ess											
							_	l Clie																
							_	l Clie																
						Ori	gina	l Clie					onti	nued										
											Revisi													
								olicy l																
								olicy l																
							Po	olicy 1				ntinu	ıed											
											e ID													
								T	unn	el l	Rule 1	D												

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										
	Rule A	Action	Rule Reason											
	Rule Reas	son, cont.	Initiato	or Port										
	Respond	ler Port	TCP I	Flags										
	Protocol		NetFlow Source											
		NetFlow Sour	rce, continued											
		NetFlow Sour	ce, continued											
		NetFlow Sour	ce, continued											
	NetFlow Src., cont.	Instan	ce ID	Connection Counter										
	Cx Ctr, cont.	First Packet Timestamp												
	First Pkt Time, cont.	I	Last Packet Timestamp											
	Last Pkt Time, cont.	Init	iator Transmitted Pack	ets										
		Initiator Transmitted	Packets, continued											
	Init. Tx Pkt, cont.	Resp	onder Transmitted Pac	kets										
		Responder Transmitte	ed Packets, continued											
	Resp. Tx Pkt, cont.	Ini	tiator Transmitted Byte	es										
		Initiator Transmitte	d Bytes, continued											
	Init. Tx Bytes, cont.	Resp	onder Transmitted Pac	kets										
		Responder Transmitt	ed Bytes, continued											
	Resp. Tx. Bytes, cont.	In	itiator Packets Droppe	d										
		Initiator Packets D	ropped, continued.											
	Init. Pkt. Drop, cont.	Res	sponder Packets Dropp	ed										
		Responder Packets I	Oropped, continued.											
	Resp. Pkt. Drop, cont.	I	nitiator Bytes Dropped											

Byte	0	1	1 2							3							
Bit	0 1 2 3 4 5 6 7	8 9 1 1	$\begin{array}{c cccc} 1 & 1 & 1 \\ 2 & 3 & 4 \end{array}$	1 1 5 6	1 7	1 1 8 9	2	$\begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix}$	2 3	2	2 2	2 6	2 7	2 8	2 9	3 3	
		Initiato	or Bytes	Drop	ped	, cont	inu	ied.									
	Init. Byte Drop, cont.	Responder Bytes Dropped															
		Responder Bytes Dropped, continued.															
	Rsp. Byte Drop, cont.		QOS Applied Interface														
		QOS A	Applied 1	Interf	ace	, cont	inu	ied									
		QOS A	Applied 1	Interf	ace	, cont	inu	ied									
		QOS A	Applied 1	Interf	ace	, cont	inu	ied									
	QOS Intf., cont.				Q	OS R	ule	e ID									
	QOS Rule ID, cont.					Use	r II	)									
	User ID, cont.			Ap	plic	ation	Pro	otoco	ol II	)							
	App Prot. ID, cont.				U	RL C	ate	gory									
	URL Category, cont.				UR	L Re	put	ation	ı								
	URL Rep., cont.			Cl	ien	t App	lica	ation	ID								
	Client App ID, cont.			V	Veb	Appl	ica	tion	ID								
	Web App. ID, cont.			S	tr. ]	Block	Ту	ype (	0)								
Client URL	Str. Block Type, cont.			S	trin	g Blo	ck	Leng	gth								
	Str. Block Len., cont.			(	Clie	nt Ap	p. l	URL									
N			String B	lock '	Тур	e (0)											
NetBIOS Name			String E	Block	Lei	ngth											
ž			NetBI	OS N	am	e											
ion			String B	lock '	Тур	e (0)											
Client App Version			String E	Block	Lei	ngth											
App		Clie	ent Appl	icatio	n V	'ersio	n										

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 3 3 4 5 6 7 8 9 0 1			
	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				
	Intrusion E	vent Count	Initiator Country				
	Responder	r Country	Original Client Country				
	IOC N	umber	Source Autono	omous System			
	Source Autonomous	System, continued	Destination Auto	nomous System			
	Destination Auto	nomous System	SNMP In				
	SNMI	? Out	Source TOS	Destination TOS			
	Source Mask	Destination Mask	Security	Context			
		Security	Context				
		Security Conte	ext, continued				
	Security Context, continued						
	Security Conte	ext, continued	VLA	N ID			
Host	String Block Type (0)						
nced ]		String Blo	ck Length				
Referenced Host	Referenced Host						

Byte Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 1 8	2 1   1   1   1   2   2   2   2   2   6   7   8   9   0   1   2   3	3 2 2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1		
	String Block Type (0)					
User Agent	String Block Length					
User	User Agent					
rer.	String Block Type (0)					
Refer		String Blo	ck Length			
HTTP Referrer		HTTP R	eferrer			
		SSL Certifica	te Fingerprint			
		SSL Certificate Fin	gerprint, continued			
		SSL Certificate Fin	gerprint, continued			
		SSL Certificate Fin	gerprint, continued			
		SSL Certificate Fin	gerprint, continued			
	SSL Policy ID					
	SSL Policy ID, continued					
		SSL Policy II	D, continued			
	SSL Policy ID, continued					
		SSL R	ule ID			
	SSL Cipl	ner Suite	SSL Version	SSL Srv Cert. Stat.		
	S	SL Srv Cert. Stat., con	i.	SSL Actual Action		
	SSL Actual SSL Expected Action SSL Flow St Action, cont.					
	SSL Flow Status, cont. SSL Flow Error					
	SSL Flow Error, continued SSL Flow Messages					
	SSL Flow SSL Flow Flags Messages, continued					
		SSL Flow Fla	gs, 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     3     3     3			
ames	SSL Flow Flags, String Block Type (0) continued					
SSL Server Names	String Block Type (0), continued String Block Length					
SSF S	String Block Length, continued		SSL Server Name			
•		SSL URL	Category			
		SSL Ses	sion ID			
		SSL Session l	D, continued			
		SSL Session l	D, continued			
		SSL Session l	D, continued			
		SSL Session l	D, continued			
		SSL Session l	D, continued			
	SSL Session ID, continued					
	SSL Session ID, continued					
	SSL Session ID Length		SSL Ticket ID			
		D, continued				
		SSL Ticket I	D, continued			
		SSL Ticket I	D, continued			
		SSL Ticket I	D, continued			
	SSL Ticket ID, cont.	SSL Ticket ID Length	Network Analysis Policy Revision			
	Network Analysis Policy Revision, continued					
	Network Analysis Policy Revision, continued					
	Network Analysis Policy Revision, continued					
	Network Analysis Policy Revision, Endpoint Profile ID continued					
	Endpoint Profile	e ID, continued	Security Group 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	
	Security Group	ID, continued	Source Security Group Tag		
	Src. Sec. Grp Tag Type	Destination Secu	urity Group Tag	Dst. Sec. Grp. Tag Type	
		Locatio	on IPv6		
		Location IPv	6, continued		
		Location IPv	6, continued		
		Location IPv	6, continued		
		HTTP R	esponse		
iery		String Bloc	ek Type (0)		
DNS Query		String Blo	ck Length		
Q	DNS Query				
	DNS Record Type DNS Response Ty				
	DNS TTL				
	Sinkhole UUID				
	Sinkhole UUID, continued				
	Sinkhole UUID, continued Sinkhole UUID, continued				
		Security Intel			
		Security Intel			
	Threat Intelligence Category				
ngres	String Block Type (0)  String Block Length  Ingress VRF Name				
s VRI	String Block Length  Ingress VRF Name				
		String Bloc			
Egress VRF		String Blo			
VRF		Egress VR			
		251000 VI			

Byte	0		1		2		3	
Bit	0 1 2 3 4	5 6 7 8	8 9 1 1	$\begin{array}{c cccc} 1 & 1 & 1 & 1 \\ 2 & 3 & 4 & 5 \end{array}$	1 1 1 6 7 8	$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	2     2     2     2     2     2     3     3       4     5     6     7     8     9     0     1	
Sou	String Block Type (0)							
Source Attr.	String Block Length							
ttr.	Source IP Dynamic Attributes							
De	String Block Type (0)							
Dest. Attr.	String Block Length							
ir.	Destination IP dynamic Attributes							

The following table describes the fields of the Connection Statistics data block for 7.0.

Table B-46 Connection Statistics Data Block 7.0 Fields

Field	Data Type	Description
Connection Statistics Data Block Type	uint32	Initiates a Connection Statistics data block for 7.0+. The value is always 173.
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.
Original Client IP Address	uint8[16]	IP address of the host behind the proxy that originated the request, 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.

Table B-46 Connection Statistics Data Block 7.0 Fields (continued)

Field	Data Type	Description
Tunnel Rule ID	uint32	Internal identifier for the tunnel 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	uint32	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.
Initiator Packets Dropped	uint64	Number of packets dropped from the session initiator due to rate limiting.
Responder Packets Dropped	uint64	Number of packets dropped from the session responder due to rate limiting.
Initiator Bytes Dropped	uint64	Number of bytes dropped from the session initiator due to rate limiting.
Responder Bytes Dropped	uint64	Number of bytes dropped from the session responders due to rate limiting.
QOS Applied Interface	uint8[16]	For rate-limited connections, the name of the interface on which rate limiting is applied.
QOS Rule ID	uint32	Internal ID number of the Quality of Service rule applied to the connection, if applicable.

Table B-46 Connection Statistics Data Block 7.0 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-46 Connection Statistics Data Block 7.0 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 block list.
Security Intelligence Layer	uint8	The IP layer that matched the IP block list.
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.
Original Client Country	uint 16	Code for the country of the host behind the proxy which originated the request.
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.
VLAN ID	uint16	VLAN identification number that indicates which VLAN the host is a member of.
String Block Type	uint32	Initiates a String data block containing the Referenced Host. This value is always 0.

Table B-46 Connection Statistics Data Block 7.0 Fields (continued)

Field	Data Type	Description	
String Block Length	uint32	The number of bytes included in the Referenced Host String data block, including eight bytes for the block type and header fields plus the number of bytes in the Referenced Host field.	
Referenced Host	string	Host name information provided in HTTP or DNS.	
String Block Type	uint32	Initiates a String data block containing the User Agent. This value is always 0.	
String Block Length	uint32	The number of bytes included in the User Agent String data block, including eight bytes for the block type and header fields plus the number of bytes in the User Agent field.	
User Agent	string	Information from the UserAgent header field in the session.	
String Block Type	uint32	Initiates a String data block containing the HTTP Referrer. This value is always 0.	
String Block Length	uint32	The number of bytes included in the HTTP Referrer String data block, including eight bytes for the block type and header fields plus the number of bytes in the HTTP Referrer field.	
HTTP Referrer	string	The site from which a page originated. This is found int he Referred header information in HTTP traffic.	
SSL Certificate Fingerprint	uint8[20]	SHA1 hash of the SSL Server certificate.	
SSL Policy ID	uint8[16]	ID number of the SSL policy that handled the connection.	
SSL Rule ID	uint32	ID number of the SSL rule or default action that handled the connection.	
SSL Cipher Suite	uint16	Encryption suite used by the SSL connection. The value is stored in decimal format. See  www.iana.org/assignments/tls-parameters/tls-parameters.  xhtml for the cipher suite designated by the value.	
SSL Version	uint8	The SSL or TLS protocol version used to encrypt the connection.	
SSL Server	uint32	The status of the SSL certificate. Possible values include:	
Certificate Status		• 0 — Not checked — The server certificate status was not evaluated.	
		• 1 — Unknown — The server certificate status could not be determined.	
		• 2 — Valid — The server certificate is valid.	
		• 4 — Self-signed — The server certificate is self-signed.	
		• 16 — Invalid Issuer — The server certificate has an invalid issuer.	
		• 32 — Invalid Signature — The server certificate has an invalid signature.	
		• 64 — Expired — The server certificate is expired.	
		• 128 — Not valid yet — The server certificate is not yet valid.	
		• 256 — Revoked — The server certificate has been revoked.	

Table B-46 Connection Statistics Data Block 7.0 Fields (continued)

Field	Data Type	Description
SSL Actual Action	uint16	The action performed on the connection based on the SSL Rule. This may differ from the expected action, as the action as specified in the rule may be impossible. Possible values include:
		• 0 — 'Unknown'
		• 1 — 'Do Not Decrypt'
		• 2 — 'Block'
		• 3 — 'Block With Reset'
		• 4 — 'Decrypt (Known Key)'
		• 5 — 'Decrypt (Replace Key)'
		• 6 — 'Decrypt (Resign)'
SSL Expected Action	uint16	The action which should be performed on the connection based on the SSL Rule. Possible values include:
		• 0 — 'Unknown'
		• 1 — 'Do Not Decrypt'
		• 2 — 'Block'
		• 3 — 'Block With Reset'
		• 4 — 'Decrypt (Known Key)'
		• 5 — 'Decrypt (Replace Key)'
		• 6 — 'Decrypt (Resign)'

Table B-46 Connection Statistics Data Block 7.0 Fields (continued)

Field	Data Type	Description
SSL Flow Status	uint16	Status of the SSL Flow. These values describe the reason behind the action taken or the error message seen. Possible values include:
		• 0 — 'Unknown'
		• 1 — 'No Match'
		• 2 — 'Success'
		• 3 — 'Uncached Session'
		• 4 — 'Unknown Cipher Suite'
		• 5 — 'Unsupported Cipher Suite'
		• 6 — 'Unsupported SSL Version'
		• 7 — 'SSL Compression Used'
		• 8 — 'Session Undecryptable in Passive Mode'
		• 9 — 'Handshake Error'
		• 10 — 'Decryption Error'
		• 11 — 'Pending Server Name Category Lookup'
		• 12 — 'Pending Common Name Category Lookup'
		• 13 — 'Internal Error'
		• 14 — 'Network Parameters Unavailable'
		• 15 — 'Invalid Server Certificate Handle'
		• 16 — 'Server Certificate Fingerprint Unavailable'
		• 17 — 'Cannot Cache Subject DN'
		• 18 — 'Cannot Cache Issuer DN'
		• 19 — 'Unknown SSL Version'
		• 20 — 'External Certificate List Unavailable'
		• 21 — 'External Certificate Fingerprint Unavailable'
		• 22 — 'Internal Certificate List Invalid'
		• 23 — 'Internal Certificate List Unavailable'
		• 24 — 'Internal Certificate Unavailable'
		• 25 — 'Internal Certificate Fingerprint Unavailable'
		• 26 — 'Server Certificate Validation Unavailable'
		• 27 — 'Server Certificate Validation Failure'
		• 28 — 'Invalid Action'
SSL Flow Error	uint32	Detailed SSL error code. These values may be needed for support purposes.

Table B-46 Connection Statistics Data Block 7.0 Fields (continued)

Field	Data Type	Description
SSL Flow Messages	uint32	The messages exchanged between client and server during the SSL handshake. See http://tools.ietf.org/html/rfc5246 for more information.
		0x00000001 — NSE_MTHELLO_REQUEST
		0x00000002 — NSE_MTCLIENT_ALERT
		• 0x00000004 — NSE_MTSERVER_ALERT
		0x00000008 — NSE_MTCLIENT_HELLO
		• 0x00000010 — NSE_MTSERVER_HELLO
		0x00000020 — NSE_MTSERVER_CERTIFICATE
		• 0x00000040 — NSE_MTSERVER_KEY_EXCHANGE
		0x00000080 — NSE_MTCERTIFICATE_REQUEST
		0x00000100 — NSE_MTSERVER_HELLO_DONE
		0x00000200 — NSE_MTCLIENT_CERTIFICATE
		• 0x00000400 — NSE_MTCLIENT_KEY_EXCHANGE
		• 0x00000800 — NSE_MTCERTIFICATE_VERIFY
		• 0x00001000 —  NSE_MTCLIENT_CHANGE_CIPHER_SPEC
		0x00002000 — NSE_MTCLIENT_FINISHED
		• 0x00004000 — NSE_MTSERVER_CHANGE_CIPHER_SPEC
		• 0x00008000 — NSE_MTSERVER_FINISHED
		0x00010000 — NSE_MTNEW_SESSION_TICKET
		• 0x00020000 — NSE_MTHANDSHAKE_OTHER
		• 0x00040000 — NSE_MTAPP_DATA_FROM_CLIENT
		• 0x00080000 — NSE_MTAPP_DATA_FROM_SERVER
SSL Flow Flags	uint64	The debugging level flags for an encrypted connection. Possible values include:
		• 0x00000001 — NSE_FLOWVALID - must be set for other fields to be valid
		0x00000002 — NSE_FLOWINITIALIZED - internal structures ready for processing
		0x00000004 — NSE_FLOWINTERCEPT - SSL session has been intercepted
String Block Type	uint32	Initiates a String data block containing the SSL Server Name. This value is always 0.

Table B-46 Connection Statistics Data Block 7.0 Fields (continued)

Field	Data Type	Description
String Block Length	uint32	The number of bytes included in the SSL Server Name String data block, including eight bytes for the block type and header fields plus the number of bytes in the SSL Server Name field.
SSL Server Name	string	Name provided in the server name indication in the SSL Client Hello.
SSL URL Category	uint32	Category of the flow as identified from the server name and certificate common name.
SSL Session ID	uint8[32]	Value of the session ID used during the SSL handshake when the client and server agree to do session reuse
SSL Session ID Length	uint8	Length of the SSL Session ID. While the session ID cannot exceed 32 bytes, it may be less than 32 bytes.
SSL Ticket ID	uint8[20]	Hash of the session ticket used when the client and server agree to use a session ticket.
SSL Ticket ID Length	uint8	Length of the SSL Ticket ID. While the ticket ID cannot exceed 20 bytes, it may be less than 20 bytes.
Network Analysis Policy revision	uint8[16]	Revision of the Network Analysis Policy associated with the connection event.
Endpoint Profile ID	uint32	ID number of the type of device used by the connection endpoint as identified by ISE. This is unique for each DC and resolved in metadata.
Security Group ID	uint32	ID number assigned to the user by ISE based on policy.
Source Security Group Tag	uint16	The Security Group Tag of the source of the connection.
Source Security Group Tag Type	uint8	How the Source Security Group Tag was assigned:
		• 0 — Unknown
		• 1 — Inline
		• 2 — Session Directory
		• 3 — Security Group Tag Exchange Protocol (SXP)
Destination Security Group Tag	uint16	The Security Group Tag of the destination of the connection.
Destination	uint8	How the Destination Security Group Tag was assigned:
Security Group Tag Type		• 0 — Unknown
		• 1 — Inline
		• 2 — Session Directory
		• 3 — Security Group Tag Exchange Protocol (SXP)
Location IPv6	uint8[16]	IP address of the interface communicating with ISE. Can be IPv4 or IPv6.
HTTP Response	uint32	Response code of the HTTP Request.

Table B-46 Connection Statistics Data Block 7.0 Fields (continued)

Field	Data Type	Description	
String Block Type	uint32	Initiates a String data block for the DNS query. 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 DNS query string.	
DNS Query	string	The content of the query sent to the DNS server.	
DNS Record Type	uint16	The numerical value for the type of DNS record.	
DNS Response Type	uint16	The numerical value for the type of DNS response.	
DNS TTL	uint32	The time to live for the DNS response, in seconds.	
Sinkhole UUID	uin8[16]	Revision UUID associated with this sinkhole object.	
Security Intelligence List 1	uint32	Security Intelligence List associated with the event. This maps to a Security Intelligence list in associated metadata. There may be three Security Intelligence lists associated with the connection.	
Security Intelligence List 2	uint32	Security Intelligence List associated with the event. This maps t a Security Intelligence list in associated metadata. There may be three Security Intelligence lists associated with the connection.	
Threat Intelligence Category	uint32	Threat Intelligence Category associated with the event. This maps to a Threat Intelligence list in associated metadata.	
String Block Type	uint32	Initiates a String data block containing the name of the ingress VRF. This value is always o.	
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 Ingress VRF name field.	
Ingress VRF Name	string	The virtual router through which traffic entered the network.	
String Block Type	uint32	Initiates a String data block containing the name of the egress VRF. This value is always 0.	
String Block Length	uint32	The number of bytes included in the name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Egress VRF name field.	
Egress VRF Name	string	The name of the virtual router through which traffic exited the network.	
String Block Type	uint32	Initiates a String data block containing the name of the Source IP Dynamic Attribute. This value is always 0.	
String Block Length	uint32	The number of bytes included in the name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Source IP Dynamic Attribute field.	

Table B-46	Connection Statistics Data Block 7.0 Fields (continued)	
I abie D-40	Connection Statistics Data Diock 7.v Fields (continued)	

Field	Data Type	Description
Source IP Dynamic Attribute	string	Dynamic Attributes associated with the source IP address.
String Block Type	uint32	Initiates a String data block containing the name of the Destination IP Dynamic Attribute. This value is always 0.
String Block Length	uint32	The number of bytes included in the name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Destination IP Dynamic Attribute field.
Destination IP Dynamic Attribute	string	Dynamic Attributes associated with the destination IP address.

# **Legacy File Event Data Structures**

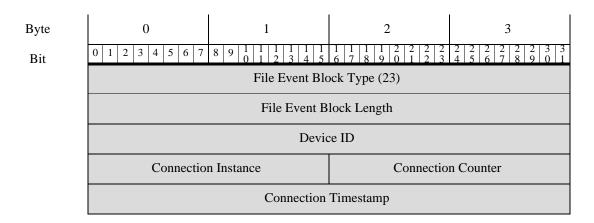
The following topics describe other legacy file event data structures:

- File Event for 5.1.1.x, page B-290
- File Event for 5.2.x, page B-294
- File Event for 5.3, page B-298
- File Event for 5.3.1, page B-304
- File Event for 5.4.x, page B-310
- File Event SHA Hash for 5.1.1-5.2.x, page B-330

## 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 1 1 1 1 1 2 2 2 2 2 2				
	File Event Timestamp				
		Source IP Address			
	Source IP Address, continued				
		Source IP Adda			
		Source IP Addi	ress, continued		
		Destination	IP Address		
		Destination IP Ac	ddress, continued		
		Destination IP Ac	ddress, continued		
		Destination IP Ac	ldress, continued		
	Disposition	Action	SHA Hash		
		SHA Hash, continued			
	SHA Hash, continued				
	SHA Hash, continued				
		SHA Hash,	continued		
		SHA Hash,	continued		
		SHA Hash,	continued		
		SHA Hash,	continued		
	SHA Hash,	continued	File Type ID		
File Name	File Type		String Block Type (0)		
	String Block T	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		

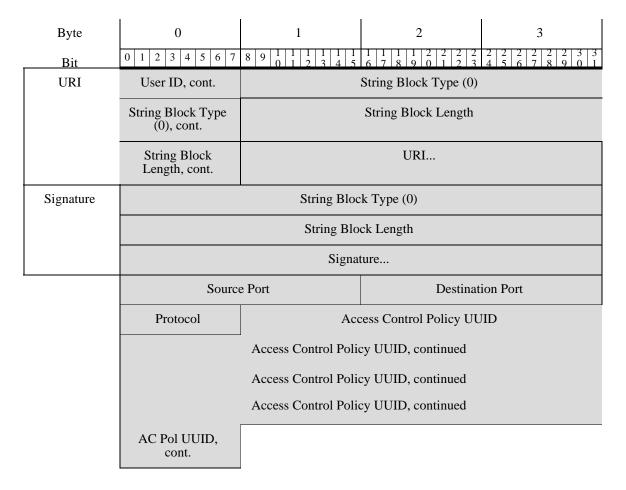


Table B-47 File Event Data Block Fields

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.

Table B-47 File Event Data Block Fields (continued)

Field	Data Type	Description	
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.	
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 Allow List	
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	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.	

Table B-47 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.

## 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 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 Instance Connection Counter			
	Connection Timestamp			
	File Event Timestamp			
	Source IP Address			
	Source IP Address, continued			
		Source IP Addr	ress, continued	
		Source IP Addr	ress, continued	

Byte	0	1	2 3	
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1 1 1	1 1 1 1 2 2 2 2 2 2 2 2 2 2 2 2 3 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0	
	Destination IP Address			
		Destination IP Ad		
		Destination IP Ad		
		Destination IP Ad	ldress, continued	
	Disposition	Action	SHA Hash	
		SHA Hash,	continued	
		SHA Hash,	continued	
		SHA Hash,	continued	
		SHA Hash,	continued	
		SHA Hash,	continued	
	SHA Hash, continued			
	SHA Hash, continued			
	SHA Hash,	continued	File Type ID	
File Name	File Type ID, cont. String Block Type (0)			
	String Block T	Type (0), cont.	String Block Length	
	String Block	Length, cont.	File Name	
		File	Size	
	File Size, continued			
	Direction Application ID			
	App ID, cont.		User ID	
URI	User ID, cont.		String Block Type (0)	
	String Block Type (0), cont.		String Block Length	
	String Block Length, cont.		URI	

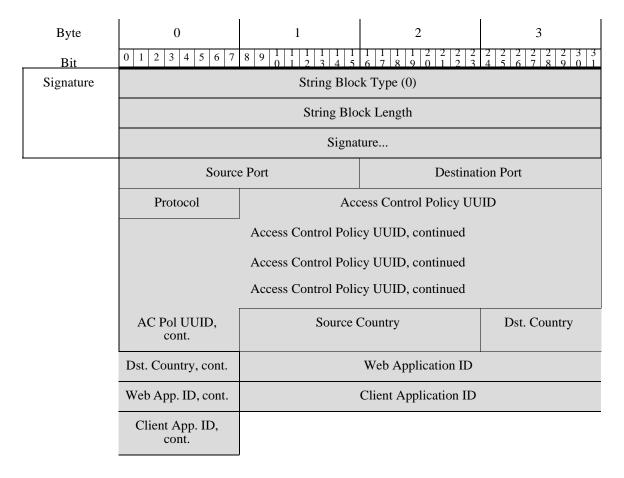


Table B-48 File Event Data Block Fields

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.	

Table B-48 File Event Data Block Fields (continued)

Field	Data Type	Description	
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 — 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 Allow List	
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	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.	

Table B-48 File Event Data Block Fields (continued)

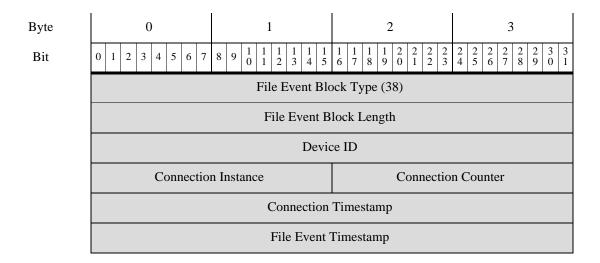
Field	Data Type	Description
Protocol	uint8	IANA protocol number specified by the user. For example:
		• 1 — ICMP
		• 4 — IP
		• 6 — TCP
		• 17 — UDP
		This is currently only TCP.
Access Control Policy UUID	uint8[16]	Unique identifier for the access control policy that triggered the event.
Source Country	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 2-13. If you enable bit 23, an extended event header is included in the record.

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



Byte	0	1	2	3
Bit	0 1 2 3 4 5 6 7	8 9 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
	Source IP Address			
		Source IP Add	ress, continued	
		Source IP Add	ress, continued	
		Source IP Add	ress, continued	
		Destination	IP Address	
		Destination IP A	ddress, continued	
		Destination IP A	ddress, continued	
		Destination IP A	ddress, continued	
	Disposition	SPERO Disposition	File Storage Status	File Analysis Status
	Archive File Status	Threat Score	Action	SHA Hash
	SHA Hash, continued			
	SHA Hash, continued			
	SHA Hash, continued			
		SHA Hash, continued		
		SHA Hash	, continued	
		SHA Hash, continued		
	SHA Hash, continued			
		SHA Hash, continued		File Type ID
File Name	File Type ID, cont.  String Block Type (0)		String Block Type (0)	
	String Block Type (0), cont.  String Block Length			
	String Block Length, cont. File Name			File Name
		File Size		
		File Size, continued		
	Direction	Direction Application ID		
	App ID, cont.		User 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
URI	User ID, cont.		String Block Type (0)	
	String Block Type (0), cont.		String Block Length	
	String Block Length, cont.		URI	
Signature		String Bloc	ek Type (0)	
		String Blo	ck Length	
	Signature			
	Source Port Destination Port		ion Port	
	Protocol	Acc	cess Control Policy UU	JID
		Access Control Police	cy UUID, continued	
		Access Control Police	cy UUID, continued	
		Access Control Police	cy UUID, continued	
	AC Pol UUID, cont.	Source (	Country	Dst. Country
	Dst. Country, cont.	. Country, cont. Web Application ID		
	Web App. ID, cont.		Client Application ID	
	Client App. ID, cont.			

Table B-49 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-49 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.	
		<ul> <li>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.</li> </ul>	
		• 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-49 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 Allow List
SHA Hash	uint8[32]	SHA-256 hash of the file, in binary format.

Table B-49 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 AMP for Endpoints File Type Metadata, page 3-38 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.	

### 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 2-13. If you enable bit 23, an extended event header is included in the record.

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

Byte	0	1 2		3		
Bit	0 1 2 3 4 5 6 7	8 9 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		
		File Event Blo	ock Type (43)			
		File Event B	lock Length			
		Device	ce ID			
	Connection	n Instance	Connectio	n Counter		
		Connection	Timestamp			
		File Event Timestamp				
	Source IP Address					
	Source IP Address, continued					
	Source IP Address, continued					
		Source IP Address, continued				
	Destination IP Address					
	Destination IP Address, continued					
	Destination IP Address, continued					
	Destination IP Address, continued					
	Disposition	SPERO Disposition	File Storage Status	File Analysis Status		
	Archive File Status	Threat Score	Action	SHA Hash		

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	
		SHA Hash,		
		SHA Hash,		
		SHA Hash,	, continued	
		SHA Hash, continued		File Type ID
File Name	File Type ID, cont.  String Block Type (0)		String Block Type (0)	
	Str	ring Block Type (0), co	nt.	String Block Length
	St	tring Block Length, cor	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 Block Type (0)			
	String Block Length			
	Signature			
	Source	e Port	Destina	tion Port
	Protocol	Acc	cess Control Policy UU	JID
	Access Control Policy UUID, continued			

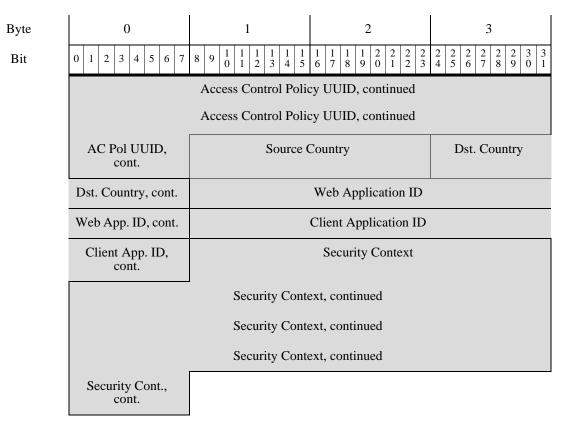


Table B-50 File Event Data Block Fields

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-50 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-50 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
		• 23 —File Transmit File Capacity Handled — File capacity handled (stored on the sensor) because file could not be submitted to the sandbox for analysis
		• 25 — File Transmit Server Limited Exceeded Capacity Handled — File capacity handled due to rate limiting on server
		• 26 — Communication Failure — File capacity handled due to cloud connectivity failure
		• 27 — Not Sent — File not sent due to configuratio
		<ul> <li>28 — Preclass No Match —File not sent for dynami analysis since pre-classification didn't find any embedded or suspicious object in the file</li> </ul>
		• 29 — Transmit Sent Sandbox Private Cloud — File sent to the private cloud for dynamic analysis
		• 30 — Transmit Not Send Sendbox Private Cloud - File not send to the private cloud for analysis

Table B-50 File Event Data Block Fields (continued)

Field	Data Type	Description	
Archive File Status	uint8	This is always o.	
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 Allow List	
SHA Hash	uint8[32]	SHA-256 hash of the file, in binary format.	
File Type ID	uint32	ID number that maps to the file type. The meaning of this field is transmitted in the metadata with this event. See AMP for Endpoints File Type Metadata, page 3-38 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.	

Table B-50 File Event Data Block Fields (continued)

Field	Data Type	Description
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 for 5.4.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 46 in the series 2 group of blocks. It supersedes block type 43. Fields for SSL and file archive support have 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 5 and an event code of 111. See Request Flags, page 2-13. If you enable bit 23, an extended event header is included in the record.

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

Byte				0	)				1			2					3															
Bit	0	1	2	3	4	5	6	7	8	9	1	1 1	1 2	1 3	1 4	1 5	1 6	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
		File Event Block Type (46)																														
		File Event Block Length																														
		Device ID																														
		Connection Instance Connection Counter																														
		Connection Timestamp																														
		File Event Timestamp																														

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			
		Source IP	Address				
		Source IP Add	ress, continued				
		Source IP Add	ress, continued				
		Source IP Add	ress, continued				
		Destination	IP Address				
		Destination IP Ac					
		Destination IP Ac					
		Destination IP Ac	ddress, continued				
	Disposition	SPERO Disposition	File Storage Status	File Analysis Status			
	Archive File Status	Threat Score	Action	SHA Hash			
		SHA Hash,	, continued				
	SHA Hash, continued						
	SHA Hash, continued						
	SHA Hash, continued						
	SHA Hash, continued						
		SHA Hash,					
	SHA Hash, continued						
		SHA Hash, continued		File Type ID			
File Name		File Type ID, cont.		String Block Type (0)			
	Str	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				

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
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	
		Signa	ture	
	Source	e Port	Destinat	tion Port
	Protocol	Acc	cess Control Policy UU	JID
		Access Control Police	cy UUID, continued	
		Access Control Police	cy UUID, continued	
		Access Control Police	cy UUID, continued	
	AC Pol UUID, cont.	Source (	Country	Dst. Country
	Dst. Country, cont.		Web Application ID	
	Web App. ID, cont.		Client Application ID	
	Client App. ID, cont.		Security Context	
		Security Conto	ext, continued	
		Security Conto	ext, continued	
		Security Conto	ext, continued	
	Security Cont., cont.	SS	L Certificate Fingerpr	int
		SSL Certificate Fin	gerprint, continued	
		SSL Certificate Fin	gerprint, continued	
		SSL Certificate Fin	gerprint, continued	
		SSL Certificate Fin	gerprint, 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 3 3 4 5 6 7 8 9 0 1						
	SSL Cert. Fpt., cont.	SSL Actu	al Action	SSL Flow Status						
Archive SHA	SSL Flow Stat., cont.	String Block Type (0)								
	Str. Blk Type, cont.	String Length								
	Str. Length, cont.	Archive SHA								
Archive Name		String Bloc	k Type (0)							
	String Block Length									
		Archive Name								
	Archive Depth									

Table B-51 File Event Data Block for 5.4.x Fields

Field	Data Type	Description
File Event Block Type	uint32	Initiates whether file event data block. This value is always 46.
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-51 File Event Data Block for 5.4.x 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.
		<ul> <li>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.</li> </ul>
		• 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-51 File Event Data Block for 5.4.x 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

Table B-51 File Event Data Block for 5.4.x Fields (continued)

Field	Data Type	Description
Archive File Status	uint8	The status of an archive being inspected. Can have the following values:
		• 0 — N/A — File is not being inspected as an archive
		• 1 — Pending — Archive is being inspected
		• 2 — Extracted — Successfully inspected without any problems
		• 3 — Failed — Failed to inspect, insufficient system resources
		<ul> <li>4 — Depth Exceeded — Successful, but archive exceeded the nested inspection depth</li> </ul>
		• 5 — Encrypted — Partially Successful, Archive was or contains an archive that is encrypted
		• 6 — Not Inspectable — Partially Successful, File is possibly Malformed or Corrupt
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 Allow List
		• 6 — Cloud Lookup Timeout
		• 7 — Custom Detection
		• 8 — Custom Detection Block
		• 9 — Archive Block (Depth Exceeded)
		• 10 — Archive Block (Encrypted)
		• 11 — Archive Block (Failed to Inspect)
SHA Hash	uint8[32]	SHA-256 hash of the file, in binary format.
File Type ID	uint32	ID number that maps to the file type. The meaning of this field is transmitted in the metadata with this event. See AMP for Endpoints File Type Metadata, page 3-38 for more information.
File Name	string	Name of the file.
File Size	uint64	Size of the file in bytes.

Table B-51 File Event Data Block for 5.4.x Fields (continued)

Field	Data Type	Description
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.
SSL Certificate Fingerprint	uint8[20]	SHA1 hash of the SSL Server certificate.

Table B-51 File Event Data Block for 5.4.x Fields (continued)

Field	Data Type	Description
SSL Actual Action	uint16	The action performed on the connection based on the SSL Rule. This may differ from the expected action, as the action as specified in the rule may be impossible. Possible values include:
		• 0 — 'Unknown'
		• 1 — 'Do Not Decrypt'
		• 2 — 'Block'
		• 3 — 'Block With Reset'
		• 4 — 'Decrypt (Known Key)'
		• 5 — 'Decrypt (Replace Key)'
		• 6 — 'Decrypt (Resign)'

Table B-51 File Event Data Block for 5.4.x Fields (continued)

Field	Data Type	Description
SSL Flow Status	uint16	Status of the SSL Flow. These values describe the
		reason behind the action taken or the error message
		seen. Possible values include:
		• 0 — 'Unknown'
		• 1 — 'No Match'
		• 2 — 'Success'
		• 3 — 'Uncached Session'
		• 4 — 'Unknown Cipher Suite'
		• 5 — 'Unsupported Cipher Suite'
		• 6 — 'Unsupported SSL Version'
		• 7 — 'SSL Compression Used'
		• 8 — 'Session Undecryptable in Passive Mode'
		• 9 — 'Handshake Error'
		• 10 — 'Decryption Error'
		• 11 — 'Pending Server Name Category Lookup'
		• 12 — 'Pending Common Name Category Lookup'
		• 13 — 'Internal Error'
		• 14 — 'Network Parameters Unavailable'
		• 15 — 'Invalid Server Certificate Handle'
		• 16 — 'Server Certificate Fingerprint Unavailable'
		• 17 — 'Cannot Cache Subject DN'
		• 18 — 'Cannot Cache Issuer DN'
		• 19 — 'Unknown SSL Version'
		• 20 — 'External Certificate List Unavailable'
		• 21 — 'External Certificate Fingerprint Unavailable'
		• 22 — 'Internal Certificate List Invalid'
		• 23 — 'Internal Certificate List Unavailable'
		• 24 — 'Internal Certificate Unavailable'
		• 25 — 'Internal Certificate Fingerprint Unavailable'
		• 26 — 'Server Certificate Validation Unavailable'
		• 27 — 'Server Certificate Validation Failure'
		• 28 — 'Invalid Action'
String Block Type	uint32	Initiates a String data block containing the Archive SHA. This value is always 0.

Table B-51 File Event Data Block for 5.4.x Fields (continued)

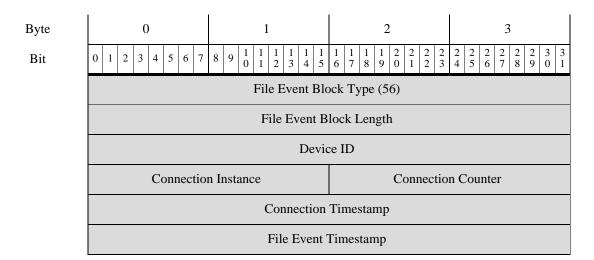
Field	Data Type	Description
String Block Length	uint32	The number of bytes included in the Archive SHA String data block, including eight bytes for the block type and header fields plus the number of bytes in the intrusion policy name.
Archive SHA	string	SHA1 hash of the parent archive in which the file is contained.
String Block Type	uint32	Initiates a String data block containing the Archive Name. This value is always 0.
String Block Length	uint32	The number of bytes included in the Archive Name String data block, including eight bytes for the block type and header fields plus the number of bytes in the intrusion policy name.
Archive Name	string	Name of the parent archive.
Archive Depth	uint8	Number of layers in which the file is nested. For example, if a text file is in a zip archive, this has a value of 1.

#### File Event for 6.x

The File Event data block 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 56 in the series 2 group of blocks. It supersedes block type 46 and is superseded by block type 79. Fields for ISE integration, file analysis, local malware analysis, and capacity handling statuses have 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 5 and an event code of 111. See Request Flags, page 2-13. If you enable bit 23, an extended event header is included in the record.

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



Byte	0	1	2	3
Bit	0 1 2 3 4 5 6 7	8 9 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
	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
	Local Malware Analysis Stat.	Archive File Status	Threat Score	Action
	SHA Hash			
	SHA Hash, continued			
	SHA Hash, continued			
	SHA Hash, continued			
	SHA Hash, continued			
	SHA Hash, continued			
	SHA Hash, continued			
		SHA Hash	, continued	
		File Ty	ype ID	
File Name	String Block Type (0)			
	String Block Length			
	File Name			
		File Size		
	File Size, continued			
	Direction		Application 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       6     7     8     9     0     1     2     3	2 2 2 2 2 3 3 4 5 6 7 8 9 0 1
	App ID, cont.		User ID	
URI	User ID, cont.	String Block Type (0)		
	String Block Type (0), cont.		String Block Length	
	String Block Length, cont.		URI	
Signature	String Block Type (0)			
	String Block Length			
	Signature			
	Source	e Port	Destinat	ion Port
	Protocol	Ac	cess Control Policy UU	JID
		Access Control Poli	cy UUID, continued	
		Access Control Poli	cy UUID, continued	
		Access Control Poli	cy UUID, continued	
	AC Pol UUID, cont.	Source	Country	Dst. Country
	Dst. Country, cont.		Web Application ID	
	Web App. ID, cont.		Client Application ID	
	Client App. ID, cont.		Security Context	
		Security Cont	ext, continued	
		Security Cont	ext, continued	
		Security Cont	ext, continued	
	Security Cont., cont.	SS	SL Certificate Fingerpr	int
		SSL Certificate Fir	ngerprint, continued	
		SSL Certificate Fir	ngerprint, continued	
		SSL Certificate Fir	ngerprint, continued	
		SSL Certificate Fir	ngerprint, 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
	SSL Cert. Fpt., cont.	SSL Actu	al Action	SSL Flow Status
Archive SHA	SSL Flow Stat., cont.		String Block Type (0)	
	Str. Blk Type, cont.	String Length		
	Str. Length, cont.	Archive SHA		
Archive Name	String Block Type (0)			
	String Block Length			
	Archive Name			
	Archive Depth	I	HTTP Response Code	
	HTTP Response Code			

Table B-52 File Event Data Block for 6.x Fields

Field	Data Type	Description	
File Event Block Type	uint32	Initiates whether file event data block. This value is always 56.	
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-52 File Event Data Block for 6.x 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.		
		<ul> <li>4 — UNAVAILABLE The software was unable to send a request to the AMP cloud for a disposition, or the AMP cloud services did not respond to the request.</li> </ul>		
		• 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-52 File Event Data Block for 6.x Fields (continued)

Field	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 Transmit File Capacity Handled — File capacity handled (stored on the sensor) because file could not be submitted to the sandbox for analysis
		• 25 — File Transmit Server Limited Exceeded Capacity Handled — File capacity handled due to rate limiting on server
		• 26 — Communication Failure — File capacity handled due to cloud connectivity failure
		• 27 — Not Sent — File not sent due to configuration
		• 28 — Preclass No Match —File not sent for dynamic analysis since pre-classification didn't find any embedded or suspicious object in the file
		• 29 — Transmit Sent Sandbox Private Cloud — File sent to the private cloud for dynamic analysis
		• 30 — Transmit Not Send Sendbox Private Cloud - File not send to the private cloud for analysis

Table B-52 File Event Data Block for 6.x Fields (continued)

Field	Data Type	Description		
Local Malware Analysis Status	uint8	The malware analysis status of the file. Possible values are:		
		• 0 — File not Analyzed		
		• 1 — Analysis Done		
		• 2 — Analysis Failed		
		• 3 — Manual Analysis Request		
Archive File Status	uint8	The status of an archive being inspected. Can have the following values:		
		• 0 — N/A — File is not being inspected as an archive		
		• 1 — Pending — Archive is being inspected		
		• 2 — Extracted — Successfully inspected without any problems		
		• 3 — Failed — Failed to inspect, insufficient system resources		
		• 4 — Depth Exceeded — Successful, but archive exceeded the nested inspection depth		
		• 5 — Encrypted — Partially Successful, Archive was or contains an archive that is encrypted		
		• 6 — Not Inspectable — Partially Successful, File is possibly Malformed or Corrupt		
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 Allow List		
		6 — Cloud Lookup Timeout		
		• 7 — Custom Detection		
		8 — Custom Detection Block		
		• 9 — Archive Block (Depth Exceeded)		
		• 10 — Archive Block (Encrypted)		
		• 11 — Archive Block (Failed to Inspect)		
SHA Hash	uint8[32]	SHA-256 hash of the file, in binary format.		

Table B-52 File Event Data Block for 6.x 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 AMP for Endpoints File Type Metadata, page 3-38 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.		

Table B-52 File Event Data Block for 6.x Fields (continued)

Field	Data Type	Description		
SSL Certificate Fingerprint	uint8[20]	SHA1 hash of the SSL Server certificate.		
SSL Actual Action	uint16	The action performed on the connection based on the SS Rule. This may differ from the expected action, as the action as specified in the rule may be impossible. Possib values include:		
		• 0 — 'Unknown'		
		• 1 — 'Do Not Decrypt'		
		• 2 — 'Block'		
		• 3 — 'Block With Reset'		
		• 4 — 'Decrypt (Known Key)'		
		• 5 — 'Decrypt (Replace Key)'		
		• 6 — 'Decrypt (Resign)'		

Table B-52 File Event Data Block for 6.x Fields (continued)

Field	Data Type	Description		
SSL Flow Status	uint16	Status of the SSL Flow. These values describe the		
		reason behind the action taken or the error message		
		seen. Possible values include:		
		• 25 — 'Internal Certificate Fingerprint Unavailable'		
		• 26 — 'Server Certificate Validation Unavailable'		
		• 27 — 'Server Certificate Validation Failure'		
		• 28 — 'Invalid Action'		
String Block Type	uint32	Initiates a String data block containing the Archive SHA. This value is always 0.		

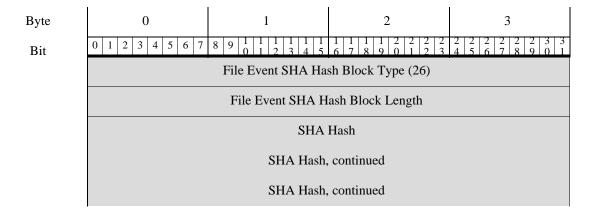
Table B-52 File Event Data Block for 6.x Fields (continued)

Field	Data Type Description				
String Block Length	uint32	The number of bytes included in the Archive SHA String data block, including eight bytes for the block type and header fields plus the number of bytes in the intrusion policy name.			
Archive SHA	string	SHA1 hash of the parent archive in which the file is contained.			
String Block Type	uint32	Initiates a String data block containing the Archive Name. This value is always 0.			
String Block Length	uint32	The number of bytes included in the Archive Name String data block, including eight bytes for the block type and header fields plus the number of bytes in the intrusion policy name.			
Archive Name	string	Name of the parent archive.			
Archive Depth	uint8	Number of layers in which the file is nested. For example, if a text file is in a zip archive, this has a value of 1.			
HTTP Response Code	uint32	HTTP Response Code			

### 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:



	SHA Hash, continued
	SHA Hash, continued
File Name	String Block Type (0)
	String Block Length
	File Name or Disposition

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

Table B-53 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.	
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.	

# **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-332
- Correlation Event for 5.1-5.3.x, page B-339

## **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 4-62.

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 V	ersion (1)	Message	Type (4)	
		Message	Length		
	Netm	ap ID	Record Ty	ype (112)	
		Record	Length		
	eStream	ner Server Timestamp (	in events, only if bit 23	3 is set)	
	Reser	rved for Future Use (in	events, only if bit 23 is	s set)	
		Correlation Blo	ock Type (116)		
	Correlation Block Length				
	Device ID				
		(Correlation)	Event Second		
		Even	t ID		
		Polic	y ID		
	Rule ID				
	Priority				
		Event Description			
		String Blo	ck Length		Description
	Description Event Type				

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	
		Event De	evice ID		
		Signatu	ıre ID		
		Signature Go	enerator ID		
		(Trigger) Ev	ent Second		
		(Trigger) Event	t Microsecond		
		Even	t ID		
		Event Defi	ned Mask		
	Event Impact Flags	IP Protocol	Network	Protocol	
		Sourc	ee IP		
	Source Host Type	Source V	LAN ID	Source OS Fprt UUID	Source OS Fprt UUID
	Source O				
	Source Criticality, cont		Source User ID		
	Source User ID, cont	Source	e Port	Source Server ID	
	Son	arce Server ID, continu	ed	Destination IP	
	Destination IP, continued Dest. Host Type				
	Dest. VLAN ID Destination OS Fingerprint UUID			ingerprint UUID	Dest OS Fingerprint
	Destination OS Fingerprint UUID, continued				ŬUÎD
		Destination OS Fingerp	orint UUID, continued		
	Destination OS F	ingerprint UUID, nued	Destination	Criticality	

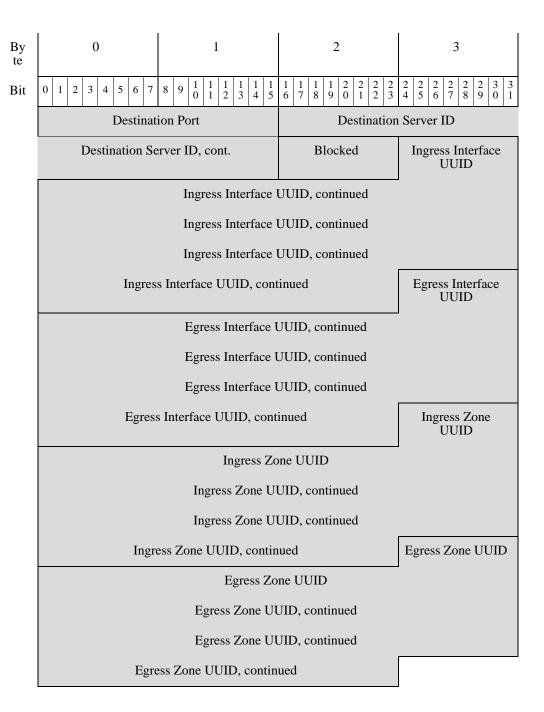


Table B-54 Correlation Event 5.0 - 5.0.2 Data Fields

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 4-62.	
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.	

Table B-54 Correlation Event 5.0 - 5.0.2 Data Fields (continued)

Field	Data Type	Description	
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 3-33 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 Service Record, page 4-15 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 Service Record, page 4-15 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 4-71.	
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 3-33 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 Secure Firewall 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.	

Table B-54 Correlation Event 5.0 - 5.0.2 Data Fields (continued)

Field	Data Type	Description	
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-55 on page B-338 for a list of each bit value.	
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 Secure Firewall 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	

Table B-54 Correlation Event 5.0 - 5.0.2 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 Service Record, page 4-15 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 Service Record, page 4-15 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.	
<b>Destination Port</b>	uint16	Destination port in the event.	
Destination Service ID	uint32	Identification number for the server running on the source host.	

Table B-54 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-55 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-55 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 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 Vo	ersion (1)	Message Type (4)		
		Message	Length		
	Netma	ap ID	Record Type (112)		
		Record	Length		
	eStream	ner Server Timestamp (i	in events, only if bit 2	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				
	Priority				

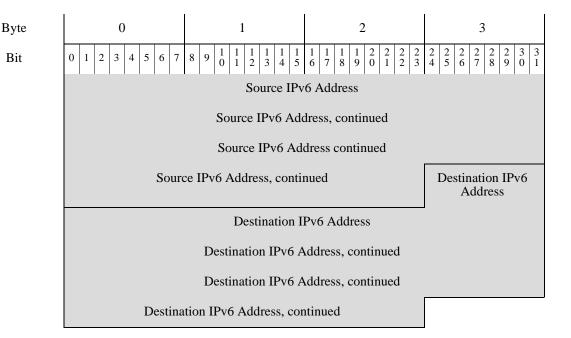
Byte

Bit

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     1     2     2     2     2     3       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 Block Type (0)				
	String Blo	ck Length		Description	
	Description		Event Type		
	Event De	evice ID			
	Signati	ure ID			
	Signature G	enerator ID			
	(Trigger) Ev	ent Second			
	(Trigger) Even	t Microsecond			
	Even	t ID			
	Event Defined Mask				
Event Impact Flags	IP Protocol	Network	Protocol		
	Source 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 Port Source Server ID		Source Server ID		
Source Server ID, continued Destination IP					
Destination IP, continued Dest. Host Type					

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 4-62.

Table B-56 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 4-62.
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 3-33 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 Service Record, page 4-15 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 Service Record, page 4-15 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-56 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 4-71.	
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 3-33 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 Secure Firewall 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-55 on page B-338 for a list of each bit value.	

Table B-56 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 Secure Firewall 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 1-4 for more information.
Source Host	uint8	Source host's type:
Type		• 0 — Host
		• 1 — Router
		• 2 — Bridge

Table B-56 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 Service Record, page 4-15 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 1-4 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 Service Record, page 4-15 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.	
<b>Destination Port</b>	uint16	Destination port in the event.	
Destination Service ID	uint32	Identification number for the server running on the source host.	

Table B-56 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 2-27 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-347
- Full Host Profile Data Block 5.1.1, page B-356
- Full Host Profile Data Block 5.2.x, page B-364
- Host Profile Data Block for 5.1.x, page B-376
- IP Range Specification Data Block for 5.0 5.1.1.x, page B-382
- Access Control Policy Rule Reason Data Block, page B-382

## 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	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	
		Full Host Profile	Data Block (111)		
		Data Blo	ck Length		
		IP Ac	ldress		
	Hops	Ger	neric List Block Type	(31)	
	Generic List Block Type, continued	G	eneric List Block Leng	gth	
OS Derived Fingerprints	Generic List Block Length, continued				
	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 Fingerprints	Operating System Fingerprint Block Type (130)*				
i mgorpinus	Operating System Fingerprint Block Length				
	Operating System Server 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 1 1 1 1 1 2 2 2 2 2 2				
Client Fingerprints	Operating System Fingerprint Block Type (130)*				
ringerprints	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)*				
Tingerprints 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)*				
1 mgerprints 2	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)*				
1 ingerprints	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 1 1 1 1 1 2 2 2 2 2 2					
Application	Operating System Fingerprint Block Type (130)*					
Fingerprints	Operating System Fin	gerprint Block Length				
	Operating System Applie	cation Fingerprint Data				
	Generic List B	lock Type (31)				
	Generic List	Block Length				
Conflict Fingerprints	Operating System Finger	rprint Block Type (130)*				
rangerprints	Operating System Fin	gerprint Block Length				
	Operating System Con	flict Fingerprint Data				
(TCP) Full Server Data	List Block	Type (11)				
Server Buttu	List Block	c Length				
	(TCP) Full Server	Data Blocks (104)*				
(UDP) Full Server Data	List Block	Type (11)				
	List Bloc	k 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 Bloc	k 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 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 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	x Type, continued	Generic List	Block Length	
Dutu	Generic List Block	Length, continued	Full Host Client Application Data Blocks (112)*		
NetBIOS Name		String Bloc	k Type (0)		
		String Bloo	ck Length		
		NetBIOS Na	me String		
Notes Data		String Bloc	k Type (0)		
		String Bloo	ck Length		
		Notes S	tring		
(VDB) Host Vulns	Generic List Block Type (31)				
		Generic List I	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 Bl	ock Type (31)		
	Generic List Block Length				
	(Third Party Scan) Host Vulnerability Data Blocks with Original Vuln IDs (85)*				
Attribute Value Data		List Block			
List Block 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-57 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.	

Table B-57 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 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 4-160 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 4-160 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 4-160 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.	

Table B-57 Full Host Profile Record 5.0 - 5.0.2 Fields (continued)

Field	Data Type	Description	
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 4-160 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 4-160 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 4-160 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 4-160 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.	

Table B-57 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 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 4-160 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 4-160 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 4-141 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 4-141 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 4-75 for a description of this data block.	

Table B-57 Full Host Profile Record 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 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 4-75 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 4-115 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 4-155 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.	

Table B-57 Full Host Profile Record 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 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 4-112 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 4-112 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 4-112 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 4-82 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	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			
	Full Host Profile Data Block (135)						
		Data Bloc	ck Length				
		IP Ad	dress				
	Hops	Ger	neric List Block Type (	31)			
	Generic List Block Type, continued	Ge	eneric List Block Leng	th			
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 Fingerprints	Operating System Fingerprint Block Type (130)*						
<i>3</i> · 1	Operating System Fingerprint Block Length						
	Operating System Server 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 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)*			
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)*			
i ingerprints i	Operating System Fingerprint Block Length			
	Operating System VDB Fingerprint Data			
		Generic List Bl	lock Type (31)	
		Generic List I	Block Length	
VDB Native Fingerprints 2	Operating System Fingerprint Block Type (130)*			
i mgerprims 2	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)*			
1 mgerprints	Operating System Fingerprint Block Length			
	Operating System User Fingerprint Data			
	Generic List Block Type (31)			
,		Generic List I	Block Length	
Scan Fingerprints	Operating System Fingerprint Block Type (130)*			
1 ingerprins	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     3     3       6     7     8     9     0     1     1     2     3     4     5     6     7     8     9     0     1			
Application Fingerprints	Operating System Fingerprint Block Type (130)*				
ringerprints	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)*				
Tingerprints	Operating System Fingerprint Block Length				
	Operating System Conflict Fingerprint Data				
(TCP) Full Server Data					
Server Buttu	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	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 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 Block Type (31)		
Host Client Data	Generic List Block Type, continued Generic			Block Length	
	Generic List Block Length, continued Full Host Client Application Data Blocks (112)*				
NetBIOS Name	String Block Type (0)				
	String Block Length				
	NetBIOS Name String				
Notes Data	String Block Type (0)				
2	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)				
Tiost vullis	Generic List Block Length				
	(Third Party/VDB) Host Vulnerability Data Blocks (85)*				
3rd Pty Scan Host Vulns	Generic List Block Type (31)				
Trost vullis	Generic List Block Length				
	(Third Party Scan) Host Vulnerability Data Blocks with Original Vuln IDs (85)*				
Attribute Value Data	List Block Type (11)				
. and Data	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-58 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 4-160 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 4-160 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 4-160 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 4-160 for a description of this data block.	

Table B-58 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 4-160 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 4-160 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 4-160 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 4-160 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-58 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 4-160 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 4-141 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 4-141 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 4-75 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 4-75 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-58 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 4-115 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 4-155 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-58 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 4-112 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 4-112 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 4-112 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 4-82 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 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 3 3 3			
		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 Fingerprints	Operating System Fingerprint Block Type (130)*			
1 mgorprints		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)*				
ringerprints	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 ingerprints 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)*				
8.1	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 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	C	Operating System Fingerprint Block Length		
	Оре	erating System Applie	cation Fingerprint Data	
		Generic List B	lock Type (31)	
		Generic List	Block Length	
Conflict Fingerprints	Оре	erating System Finger	rprint Block Type (130)	)*
imgorprima	C	Operating System Fin	gerprint Block Length	
	0	perating System Con	flict Fingerprint Data	
		Generic List B	lock Type (31)	
		Generic List	Block Length	
Mobile Fingerprints	Operating System Fingerprint Block Type (130)*			
8 1	Operating System Fingerprint Block Length			
	Operating System Mobile Fingerprint Data			
	Generic List Block Type (31)			
		Generic List	Block Length	
IPv6 Server Fingerprints	Оре	erating System Finger	rprint Block Type (130)	)*
	C	Operating System Fin	gerprint Block Length	
	Operating System IPv6 Server Fingerprint Data			
		Generic List B	lock Type (31)	
		Generic List	Block Length	
Ipv6 Client Fingerprints	Operating System Fingerprint Block Type (130)*			
	C	Operating System Fin	gerprint Block Length	
	Оре	erating System Ipv6	Client 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     3     3       6     7     8     9     0     1     1     2     3     4     5     6     7     8     9     0     1				
Ipv6 DHCP Fingerprints	Operating System Fingerprint Block Type (130)*					
Tingerprints	Operating System Fin	gerprint Block Length				
	Operating System IPv6 I	OHCP Fingerprint Data				
	Generic List B	lock Type (31)				
	Generic List	Block Length				
User Agent Fingerprints	Operating System Finger	rprint Block Type (130)*				
8.1	Operating System Fin	gerprint Block Length				
	Operating System User	Agent Fingerprint Data				
(TCP) Full Server Data	List Block	Туре (11)				
	List Block	c 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					
		ol Data Blocks (4)*				
Transport Protocol Data		Type (11)				
	List Block Length					
24.6	-	ol Data Blocks (4)*				
MAC Address Data	List Block Type (11)					
	List Block Length					
	Host MAC Address					
		Seen				
	Host					
	Business Criticality	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 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	k Type, continued	Generic List	Block Length	
Duiu	Generic List Block	Length, continued	Full Host Client App (11	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 Blo	ck Length		
	Notes String				
(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 B	lock Type (31)		
	Generic List Block Length				
	(Third Party/VDB) Host Vulnerability Data Blocks (85)*			s (85)*	
3rd Pty Scan Host Vulns	Generic List Block Type (31)				
		Generic List I	Block Length		
	(Third Party Scan	) Host Vulnerability Da	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-59 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 4-97 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 4-160 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 4-160 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 4-160 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-59 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 4-160 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 4-160 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 4-160 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 4-160 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-59 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 4-160 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 4-160 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 4-160 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 4-160 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-59 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 4-160 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 4-160 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 4-160 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 4-141 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 4-141 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-59 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 4-75 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 4-75 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 4-115 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-59 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 4-155 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 o.	
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 4-112 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 4-112 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 4-112 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-59 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 4-82 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 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 Block Type (132)			
	Host Profile Block Length			
		IP Ad	dress	
Server Fingerprints	Hops	Primary/Secondary	Generic List Block Type (31)	
1 ingerprints	Generic List Block	k Type, continued	Generic List Block Length	
	Generic List Block Length, continued Server Fingerprint Data Blocks*		int Data Blocks*	
Client Fingerprints	Generic List Block Type (31)			
Generic List Block Length			Block Length	
	Client Fingerprint Data Blocks*			
SMB Fingerprints				
1 ingorprints				
		SMB Fingerprin	t Data Blocks*	

Byte	0	1	2	3		
Bit	0 1 2 3 4 5 6 7					
DHCP Fingerprints						
ringerprints	Generic List Block Length					
		DHCP Fingerp	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 Block	x Type (11)		List of TCP Servers	
Block		List Blo	ck Length		Bervers	
		TCP Server	Data Blocks			
UDP Server Block*		List of UDP Servers				
Brock						
	UDP Server Data Blocks					
Network Protocol		List of Network Protocols				
Block*						
Transport Protocol		List Block	x Type (11)		List of Transport	
Block*		List Block Length				
MAC Address Block*		List Block Type (11)			List of MAC Addresses	
210011	List Block Length				1100108808	
	Host MAC Address Data Blocks					
		Host Last Seen				
		Host Type				
	Mobile	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     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					
rume					

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

Table B-60 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 4-160 for a description of this data block.	

Table B-60 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 4-160 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 4-160 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 4-160 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-60 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 4-160 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 4-75 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 4-75 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.	

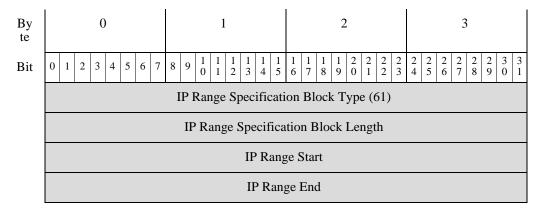
Table B-60 Host Profile Data Block 5.1.x Fields (continued)

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 4-115 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 4-155 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-61 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.

## **Access Control Policy Rule Reason Data Block**

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

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

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     3       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 Policy Rule Reason Data Block Type (21)			
	Access Control Policy Rule Reason Data Block Length			
Description	Reason		String Block Type (0)	
	String Block Type (0), continued		String Block Length	
	String Block Length, continued		Description	

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

Table B-62 Access Control Policy Rule Reason Data Block Fields

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

Legacy Host Data Structures