

Understanding Legacy Data Structures

This appendix contains information about data structures supported by eStreamer at previous versions of Firepower 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 Firepower 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-46
- Legacy Discovery Data Structures, page B-88
- Legacy Connection Data Structures, page B-123
- Legacy Correlation Event Data Structures, page B-236
- Legacy Host Data Structures, page B-251

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 Impact Alert Data, page B-44

Intrusion Event (IPv4) Record 5.0.x - 5.1

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

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

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

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

By te	0	1	2	3						
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1						
	VLA	N ID	Pa	ad						
	Policy UUID									
	Policy UUID, continued									
	Policy UUID, continued									
	Policy UUID, continued									
		User	r ID							
		Web Appl	ication ID							
		Client App	lication 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							
		Interface Egress 1	UUID, continued							
		Security Zone	Ingress UUID							
		Security Zone Ingre								
		Security Zone Ingres	ss UUID, continued							

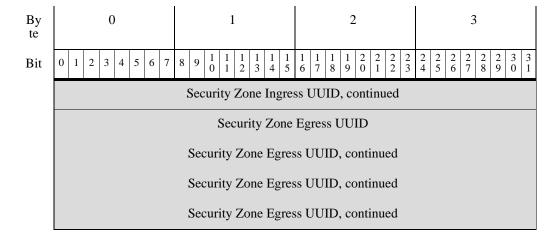


Table B-1 Intrusion Event (IPv4) Record Fields

Field	Data Type	Description
Device ID	unit32	Contains the identification number of the detecting managed device. You can obtain the managed device name by requesting Version 3 or 4 metadata. See Managed Device Record Metadata, page 3-34 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 Firepower System preprocessor that generated the event.
Rule Revision	uint32	Rule revision number.
Classification ID	uint32	Identification number of the event classification message.
Priority ID	uint32	Identification number of the priority associated with the event.
Source IPv4 Address	uint8[4]	Source IPv4 address used in the event, in address octets.
Destination IPv4 Address	uint8[4]	Destination IPv4 address used in the event, in address octets.
Source Port	uint16	The source port number if the event protocol type is TCP or UDP.
Destination Port	uint16	The destination port number if the event protocol type is TCP or UDP.

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

Field	Data Type	Description							
IP Protocol	uint8	IANA-specified protocol number. For example:							
Number		• 0 — IP							
		• 1 — ICMP							
		• 6 — TCP							
		• 17 — UDP							
Impact Flags	bits[8]	Impact flag value of the event. The low-order eight bits indicate the impact level. Values are:							
		• 0x01 (bit 0) — Source or destination host is in a network monitored by the system.							
		• 0x02 (bit 1) — Source or destination host exists in the network map.							
		• 0x04 (bit 2) — Source or destination host is running a server on the port in the event (if TCP or UDP) or uses the IP protocol.							
		• 0x08 (bit 3) — There is a vulnerability mapped to the operating system of the source or destination host in the event.							
		• 0x10 (bit 4) — There is a vulnerability mapped to the server detected in the event.							
		• 0x20 (bit 5) — The event caused the managed device to drop the session (used only when the device is running in inline, switched, or routed deployment). Corresponds to blocked status in the Firepower System web interface.							
		• 0x40 (bit 6) — The rule that generated this event contains rule metadata setting the impact flag to red. The source or destination host is potentially compromised by a virus, trojan, or other piece of malicious software.							
									• 0x80 (bit 7) — There is a vulnerability mapped to the client detected in the event.
		The following impact level values map to specific priorities on the Defense Center. An x indicates the value can be 0 or 1:							
		• (0, unknown): 00x00000							
		• red (1, vulnerable): xxxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx							
		• orange (2, potentially vulnerable): 00x00111							
		• yellow (3, currently not vulnerable): 00x00011							
		• blue (4, unknown target): 00x00001							

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

Field	Data Type	Description			
Impact	uint8	Impact flag value of the event. Values are:			
		• 1 — Red (vulnerable)			
		• 2 — Orange (potentially vulnerable)			
		• 3 — Yellow (currently not vulnerable)			
		• 4 — Blue (unknown target)			
		• 5 — (unknown impact)			
Blocked	uint8	Value indicating whether the event was blocked.			
		• 0 — Not blocked			
		• 1 — Blocked			
		• 2 — Would be blocked (but not permitted by configuration)			
MPLS Label	uint32	MPLS label.			
VLAN ID	uint16	Indicates the ID of the VLAN where the packet originated.			
Pad	uint16	Reserved for future use.			
Policy UUID	uint8[16]	A policy ID number that acts as a unique identifier for the intrusion policy.			
User ID	uint32	The internal identification number for the user, if applicable.			
Web Application ID	uint32	The internal identification number for the web application, if applicable.			
Client Application ID	uint32	The internal identification number for the client application, if applicable.			
Application Protocol ID	uint32	The internal identification number for the application protocol, if applicable.			
Access Control Rule ID	uint32	A rule ID number that acts as a unique identifier for the access control rule.			
Access Control Policy UUID	uint8[16]	A policy ID number that acts as a unique identifier for the access control policy.			
Ingress Interface UUID	uint8[16]	An interface ID number that acts as a unique identifier for the ingress interface.			
Egress Interface UUID	uint8[16]	An interface ID number that acts as a unique identifier for the egress interface.			
Ingress Security Zone UUID	uint8[16]	A zone ID number that acts as a unique identifier for the ingress security zone.			
Egress Security Zone UUID	uint8[16]	A zone ID number that acts as a unique identifier for the egress security zone.			

Intrusion Event (IPv6) Record 5.0.x - 5.1

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

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

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

By te	0	1	2	3					
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 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 V	ersion (1)	Message	Type (4)					
		Message	Length						
	Netm	ap ID	Record T	ype (208)					
		Record	Length						
	eStream	ner Server Timestamp (in events, only if bit 2	3 is set)					
	Reser	rved for Future Use (in	events, only if bit 23 i	s set)					
		Devid	ce ID						
	Event ID								
	Event Second								
	Event Microsecond								
		Rule ID (Sig	gnature ID)						
		Genera	tor ID						
		Rule Re	evision						
		Classific	ation ID						
		Priori	zy ID						
		Source IPv	6 Address						
		Source IPv6 Add	lress, continued						
		Source IPv6 Add	lress, continued						
	Source IPv6 Address, continued								
	Destination IPv6 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 2	1 1 3 4	1 5	1 1 6 7	1 1 8 9	2 0	2	2 2 3	2 4	2 2 5 6	2 7	2 8 9	3 3 0 1
		Dest	inatio	n IPv	6 A	ddres	s, co	ntin	ued	•					
	Source Port/ICMP Type Destination Port/ICMP Code														
	IP Protocol ID	Imp	act Fl	ags			Im	pact	t			В	locl	ked	
				MP	LS	Label	-								
	VLAN ID Pad														
				Pol	icy	UUID)								
			Poli	cy U	UID), con	tinue	d							
			Poli	cy U	UIC), con	tinue	d							
			Poli	cy U	UID), cont	tinue	d							
				J	Jser	· ID									
			W	eb A	ppli	ication	ı ID								
			Cli	ent A	(pp	licatio	n ID	1							
			App	licati	on	Protoc	col II	D							
			Acc	ess C	ont	rol Ru	ıle II)							
		F	Access	s Con	trol	Polic	y Ul	JID)						
		Acces	s Con	trol P	olic	y UU	ID,	cont	inue	ed					
		Acces	s Con	trol P	olic	y UU	ID,	cont	inue	ed					
		Acces	s Con	trol P	olic	y UU	ID,	cont	inu	ed					
						gress I									
		Inte	rface	Ingre	ess l	UUID	, cor	ıtinı	ied						
	Interface Ingress UUID, continued														
		Inte	rface						ied						
	Interface Egress UUID														
			erface												
		Inte	erface	Egre	ss U	JUID.	, con	tinu	ied						

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

Table B-2 Intrusion Event (IPv6) Record Fields

Field	Data Type	Description
Device ID	unit32	Contains the identification number of the detecting device. You can obtain the managed device name by requesting Version 3 or 4 metadata. See Managed Device Record Metadata, page 3-34 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 Firepower 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.			
		• 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 Firepower 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 I	Length					
		Devic	ee ID					
		Even	t ID					
		Event S	Second					
		Event Mic	rosecond					
		Rule ID (Sig	gnature ID)					
	Generator ID							
	Rule Revision							
	Classification ID							
		Priori	ty ID					

Byte	0 1		2 3					
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 3 3 3 6 7 8 9 0 1 1 2 3 4 5 6 7 8 9 0 1					
	Source IP Address							
	Source IP Address, continued							
		Source IP Add	ress, continued					
		Source IP Add	ress, continued					
		Destination	IP Address					
		Destination IP A	ldress, continued					
		Destination IP A						
		Destination IP Ac	ldress, continued					
	Source Port of	r ICMP Type	Destination Por	t or ICMP Code				
	IP Protocol ID	Impact Flags	Impact	Blocked				
		MPLS	Label					
	VLA	N ID	Pa	ad				
	Policy UUID							
	Policy UUID, continued							
	Policy UUID, continued							
	Policy UUID, continued							
	User ID							
		Web Appl	ication ID					
		Client App	lication ID					
	Application Protocol ID							
		Access Con	trol Rule ID					
	Access Control Policy UUID							
		Access Control Police	cy UUID, continued					
	Access Control Policy UUID, continued							
		Access Control Police	cy UUID, continued					
		Interface In	gress UUID					

Byte	0	1	2	3		
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1		
		Interface Ingress	UUID, continued			
		Interface Ingress	UUID, continued			
		Interface Ingress	UUID, continued			
		Interface Eg	ress UUID			
		Interface Egress I	JUID, continued			
		Interface Egress I	JUID, continued			
	Interface Egress UUID, continued					
	Security Zone Ingress UUID					
	Security Zone Ingress UUID, continued					
	Security Zone Ingress UUID, continued					
	Security Zone Ingress UUID, continued					
		Security Zone	Egress UUID			
	Security Zone Egress UUID, continued					
	Security Zone Egress UUID, continued					
	Security Zone Egress UUID, continued					
	Connection Timestamp					
	Connection	Instance ID	Connectio	n Counter		
	Source (Country	Destinatio	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 3-34 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 Firepower System preprocessor that generated the event.		
Rule Revision	uint32	Rule revision number.		
Classification ID	uint32	Identification number of the event classification message.		
Priority ID	uint32	Identification number of the priority associated with the event.		
Source IP Address	uint8[16]	Source IPv4 or IPv6 address used in the event.		
Destination IP Address	uint8[16]	Destination IPv4 or IPv6 address used in the event.		
Source Port or ICMP Type	uint16	The source port number if the event protocol type is TCP or UDP, or the ICMP type if the event is caused by ICMP traffic.		
Destination Port or ICMP Code	uint16	The destination port number if the event protocol type is TCP or UDP, or the ICMP code if the event is caused by ICMP traffic.		
IP Protocol Number	uint8	IANA-specified protocol number. For example: • 0 — IP • 1 — ICMP • 6 — TCP		
,		• 17 — UDP		

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

Field	Data Type	Description
Impact Flags	bits[8]	Impact flag value of the event. The low-order eight bits indicate the impact level. Values are:
		• 0x01 (bit 0) — Source or destination host is in a network monitored by the system.
		• 0x02 (bit 1) — Source or destination host exists in the network map.
		• 0x04 (bit 2) — Source or destination host is running a server on the port in the event (if TCP or UDP) or uses the IP protocol.
		• 0x08 (bit 3) — There is a vulnerability mapped to the operating system of the source or destination host in the event.
		• 0x10 (bit 4) — There is a vulnerability mapped to the server detected in the event.
		• 0x20 (bit 5) — The event caused the managed device to drop the session (used only when the device is running in inline, switched, or routed deployment). Corresponds to blocked status in the Firepower 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	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					
	Netm	ap ID	Record Ty	ype (400)		
		Record I	Length			
	eStrean	ner Server Timestamp (i	n events, only if bit 23	3 is set)		
	Rese	rved for Future Use (in	events, only if bit 23 is	s set)		
		Block Ty	pe (41)			
	Block Length					
	Device ID					
	Event ID					
	Event Second					
	Event Microsecond					
	Rule ID (Signature ID)					
		Generator ID				
		Rule Re	vision			
		Classifica	ation ID			
	Priority ID					
	Source IP Address					
	Source IP Address, continued					
		Source IP Addre				
		Source IP Addre	ess, continued			

Byte	0 1			2 3			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 7			2 2 2 4 5 6	$\begin{array}{c cccc} 2 & 2 & 2 & 2 \\ 5 & 7 & 8 & 9 \end{array}$	3 3 0 1
	Destination IP Address								
	Destination IP Address, continued								
		Destination IP Address, continued							
		Destir	nation IP	Addres	ss, contin	ued			
	Source Port o	r ICMP Ty _l	pe		Destin	ation Por	t or ICM	IP Code	
	IP Protocol ID	Impact	t Flags		Impa	et	I	Blocked	
			MPl	LS Lab	el				
	VLA	N ID				Pa	ad		
			Poli	ey UUI	D				
		P	Policy UU	JID, co	ntinued				
		P	Policy UU	JID, co	ntinued				
		P	Policy UU	JID, co	ntinued				
		User ID							
	Web Application ID								
	Client Application ID								
		Application Protocol ID							
			Access Co						
			cess Cont						
		Access C							
		Access C							
		Access Control Policy UUID, continued Interface Ingress UUID							
				_		uod			
		Interface Ingress UUID, continued							
	Interface Ingress UUID, continued Interface Ingress UUID, continued								
			Interface			ucu			
			incriace	LEICSS					

Byte	0	1	2	3				
Bit	0 1 2 3 4 5 6 7 8	9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1				
		Interface Egress I	JUID, continued					
		Interface Egress UUID, continued						
		Interface Egress I	UUID, continued					
		Security Zone	Ingress UUID					
		Security Zone Ingres	ss UUID, continued					
	Security Zone Ingress UUID, continued							
	Security Zone Ingress UUID, continued							
	Security Zone Egress UUID							
	Security Zone Egress UUID, continued							
	Security Zone Egress UUID, continued							
	Security Zone Egress UUID, continued							
	Connection Timestamp							
	Connection Instance ID Connection Counter							
	Source Country Destination Country							
	IOC Nur	nber						

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 3-34 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 Firepower 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 Firepower 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): 00x00001x
		• 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-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	8 9 1 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1									
	Header V	ersion (1)	Message Type (4)										
	Message Length												
	Netmap ID Record Type (400)												
		Record	Length										
	eStream	ner Server Timestamp (in events, only if bit 2	3 is set)									
	Resei	ved for Future Use (in	events, only if bit 23 i	s set)									
		Block Ty	7pe (25)										
		Block I	ength										
		Devic	e ID										
		Even	t ID										
		Event S	econd										
		Event Mic	rosecond										
		Rule ID (Sig	gnature ID)										
		Genera	tor ID										
		Rule Re	evision										
		Classific	ation ID										
		Priori	ty ID										
		Source IP	Address										
		Source IP Addr	ess, continued										
		Source IP Addr	ess, continued										
		Source IP Addr	ess, continued										

By te

Bit

0	1	2	3											
0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	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 Address												
Destination IP Address, continued														
Destination IP Address, continued														
Destination IP Address, continued														
Source Port/l	ICMP Type	Destination Port/ICMP Code												
IP Protocol ID	Impact Flags	Impact	Blocked											
	MPLS	Label												
VLA	N ID	Pa	d											
	Policy	UUID												
	Policy UUID	, continued												
	Policy UUID	, continued												
	Policy UUID	, continued												
	User	ID												
	Web Appli	cation ID												
	Client Appl	ication ID												
	Application 1	Protocol ID												
	Access Cont	rol Rule ID												
	Access Control	Policy UUID												
	Access Control Police	y UUID, continued												
	Access Control Police	y UUID, continued												
	Access Control Police	y UUID, continued												
	Interface Ing	gress UUID												
	Interface Ingress U	JUID, continued												
	Interface Ingress U	JUID, continued												
	Interface Ingress U	JUID, continued												

By te	0		1				2									3							
Bit	0 1 2 3 4 5 6 7	8 9 1		1 3		1 1 4 5	1 6	1 7	1	1 9	2	2	2 2	2 3	2 4	2 5	2 6	2 7	2 8	2 9	3	3	
			In	ter	fac	e E	gre	ss U	U	ID													
		Int	erfac	e I	Egr	ess	UU	ID,	co	ont	inı	ued											
		Int	erfac	e I	Egr	ess	UU	ID,	co	ont	inı	ued											
		Int	erfac	e F	Egr	ess	UU	ID,	co	ont	inı	ued											
			Secu	rity	y Z	Cone	Ing	gres	s U	JU	ID)											
		Secur	ity Z	on	e I	ngre	ss	UUI	D	, co	ont	tinu	ed										
		Secur	ity Z	on	e I	ngre	ss	UUI	D	, co	ont	tinu	ed										
		Secur	ity Z	on	e I	ngre	ss	UUI	D	, co	ont	tinu	ed										
			Secu	rit	y Z	Zone	Εg	res	i U	JU.	ID)											
		Secur	ity Z	Zon	e I	Egre	ss I	JUI	D,	, cc	ont	tinu	ed										
		Secur	ity Z	Zon	e I	Egre	ss I	JUI	D,	, cc	ont	tinu	ed										
		Secur	ity Z	Con	e I	Egre	ss I	JUI	D,	, cc	ont	tinu	ed										
			C	onr	nec	tion	Ti	mes	taı	mp													
	Connection	Instance	ID								С	Conr	nect	ioı	n C	ou	nte	r					

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 3-34 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 Firepower 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 Firepower 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	1 2	3	4 5		6 7	8	ç	$\frac{1}{0}$	1 1		1 1 2 3	1 4	1 5	1	1 5 7	1 8	3	1 2	2	2 2	2 3	2 4	2 5	2 6	2 7	2	2 2 9	3	3
				Hea	ıd	er V	ers	io	n (1)									l	Мe	ssa	ge	Ту	pe	(4))				
												M	ess	ag	e I	Len	gth	1												
					N	letm	ap	Η)										F	Rec	orc	l T	ype	e (400)				
	Record Length eStreamer Server Timestamp (in events, only if bit 23 is set)																													
	Reserved for Future Use (in events, only if bit 23 is set)																													
	Block Type (42)																													
	Block Length																													
	Device ID																													
	Event ID																													
	Event Second																													
												Eve	nt l	Mi	icr	oseo	cor	nd												
											R	ule	ID	(S	igı	natu	re	ID))											
																or II														
																isic														
												Cl				tion)												
																ID														
										Cor						Add				1										
												ce I																		
												ce I																		
											_																			
									De			esti atior								ıad										
												atior																		
												ation																		

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 Port of	r ICMP Type	Destination Port	or ICMP Code									
	IP Protocol ID	Impact Flags	Impact	Blocked									
		MPLS	Label										
	VLA	N ID	Pa	ıd									
	Policy UUID												
	Policy UUID, continued												
	Policy UUID, continued												
	Policy UUID, continued												
	User ID												
	Web Application ID												
	Client Application ID												
		Application	Protocol ID										
		Access Cont	rol Rule ID										
		Access Control	Policy UUID										
		Access Control Police	cy UUID, continued										
		Access Control Police	cy UUID, continued										
		Access Control Police	cy UUID, continued										
		Interface Ing	gress UUID										
		Interface Ingress	UUID, continued										
		Interface Ingress	UUID, continued										
		Interface Ingress	UUID, continued										
		Interface Eg	gress UUID										
		Interface Egress V	JUID, continued										
		Interface Egress V	JUID, continued										
		Interface Egress V	JUID, continued										
		Security Zone	Ingress UUID										

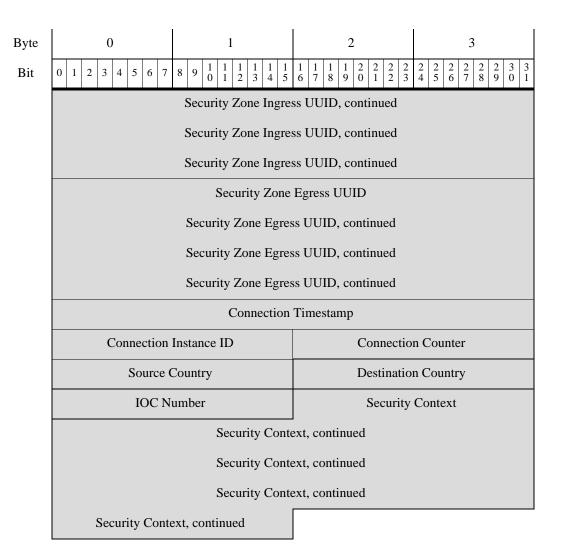


Table B-6 Intrusion Event Record 5.3.1 Fields

Field	Data Type	Description
Block Type	unint32	Initiates an Intrusion Event data block. This value is always 42.
Block Length	unint32	Total number of bytes in the Intrusion Event data block, including eight bytes for the Intrusion Event block type and length fields, plus the number of bytes of data that follows.
Device ID	unit32	Contains the identification number of the detecting managed device. You can obtain the managed device name by requesting Version 3 or 4 metadata. See Managed Device Record Metadata, page 3-34 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 Firepower System preprocessor that generated the event.
Rule Revision	uint32	Rule revision number.
Classification ID	uint32	Identification number of the event classification message.
Priority ID	uint32	Identification number of the priority associated with the event.
Source IP Address	uint8[16]	Source IPv4 or IPv6 address used in the event.
Destination IP Address	uint8[16]	Destination IPv4 or IPv6 address used in the event.
Source Port or ICMP Type	uint16	The source port number if the event protocol type is TCP or UDP, or the ICMP type if the event is caused by ICMP traffic.
Destination Port or ICMP Code	uint16	The destination port number if the event protocol type is TCP or UDP, or the ICMP code if the event is caused by ICMP traffic.
IP Protocol Number	uint8	IANA-specified protocol number. For example: • 0 — IP
		• 1 — ICMP
		• 6—TCP
		• 17 — UDP

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

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

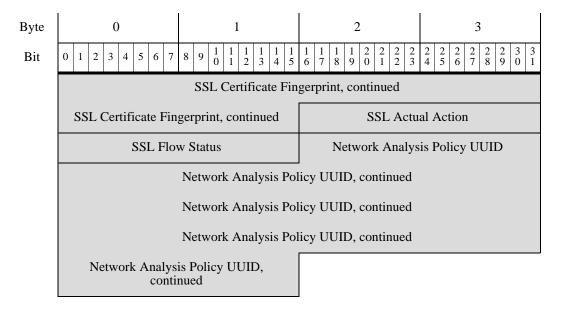
The fields in the intrusion event record are shaded in the following graphic. The record type is 400 and the block type is 45 in the series 2 set of data blocks. It supersedes block type 42, and is superseded by block type 60. Fields for SSL support and Network Analysis Policy have been added.

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			2 3				3											
Bit	0 1 2 3 4	5	6	7 8		1 1 0 1		1 1 2 3		1 5		1 7	1 8	1 2		2 2 2	2 2 3	2 4	1	2 2 5 6		2 2	2 2 9		3
	Source IP Address																								
	Source IP Address, continued																								
	Source IP Address, continued Source IP Address, continued																								
	Destination IP Address																								
														ntin											
														ntin											
					С	esti	na	atıor	ı IP	A	Add	ress	, cc	ntin	u	ed									
	Sour	ce l	Port	or I	CMI	РТу	pe	e					De	estin	at	ion	Por	t c	r I	ICM	ſΡ	Co	ode		
	IP Protoco	ol I	D		In	npac	t l	Flag	gs				Iı	npa	ct					F	Blo	ck	ed		
									MP	LS	SL	abe	1												
			VL	AN	ID												P	ad							
]	Poli	icy	y U	UII)												
						I	Po	olicy	/ UI	UI	ID,	con	tinı	ied											
						I	Po	olicy	/ UI	UI	ID,	con	tinı	ied											
						I	Po	olicy	/ UI	UI	ID,	con	tinı	ied											
									ι	Jse	er I	D													
							_	Wel	b A	pp	olica	atio	n II)											
							C	Clier	nt A	p	plic	atio	on I	D											
							Aı	ppli	cati	or	n Pr	oto	col	ID											
								cces																	
														JUII											
					Acc						-														
					Acc						-														
					Acc										nti	inue	d								
							In	iterf	ace	Ir	ngre	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 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1							
	Interface Ingress UUID, continued								
	Interface Ingress UUID, continued								
	Interface Ingress UUID, continued								
	Interface Egress UUID								
	Interface Egress UUID, continued								
	Interface Egress UUID, continued								
	Interface Egress UUID, continued								
	Security Zone	Ingress UUID							
	Security Zone Ingre	ss UUID, continued							
	Security Zone Ingre	ss UUID, continued							
	Security Zone Ingre	ss UUID, continued							
	Security Zone	Egress UUID							
	Security Zone Egress UUID, continued								
	Security Zone Egree	ss UUID, continued							
	Security Zone Egree	ss UUID, continued							
	Connection	Timestamp							
	Connection Instance ID	Connection Counter							
	Source Country	Destination Country							
	IOC Number	Security Context							
	Security Conto								
	Security Context, continued								
	Security Context, continued								
	Security Context, continued SSL Certificate Fingerprint SSL Certificate Fingerprint, continued								
	SSL Certificate Fin								
	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 metadata. See Managed Device Record Metadata, page 3-34 for mor 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 Firepower 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 Firepower 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 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 4-60.)

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

Byte	0	1	2	3					
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 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 Vo	ersion (1)	Message	Type (4)					
		Message	Length						
	Netma	ap ID	Record Type (9)						
		Record	Length						
		Intrusion Impact Ale	ert Block Type (20)						
		Intrusion Impact A	lert Block Length						
	Event ID								
	Device ID								
		Event S	Second						
		Imp	act						
		Source IP	Address						
		Destination	IP Address						
Impact Description									
Description	String Block Length								
	Description								

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

Table B-8 Impact Event Data Fields

Field	Data Type	Description
Intrusion Impact Alert Block Type	uint32	Indicates that an intrusion impact alert data block follows. This field will always have a value of 20. See Intrusion Event and Metadata Record Types, page 3-1.
Intrusion Impact Alert Block Length	uint32	Indicates the length of the intrusion impact alert data block, including all data that follows and 8 bytes for the intrusion impact alert block type and length.
Event ID	uint32	Indicates the event identification number.
Device ID	uint32	Indicates the managed device identification number.
Event Second	uint32	Indicates the second (from 01/01/1970) that the event was detected.
Impact	bits[8]	Impact flag value of the event. The low-order eight bits indicate the impact level. Values are:
		• 0x01 (bit 0) — Source or destination host is in a network monitored by the system.
		• 0x02 (bit 1) — Source or destination host exists in the network map.
		• 0x04 (bit 2) — Source or destination host is running a server on the port in the event (if TCP or UDP) or uses the IP protocol.
		• 0x08 (bit 3) — There is a vulnerability mapped to the operating system of the source or destination host in the event.
		• 0x10 (bit 4) — There is a vulnerability mapped to the server detected in the event.
		• 0x20 (bit 5) — The event caused the managed device to drop the session (used only when the device is running in inline, switched, or routed deployment). Corresponds to blocked status in the Firepower System web interface.
		• 0x40 (bit 6) — The rule that generated this event contains rule metadata setting the impact flag to red. The source or destination host is potentially compromised by a virus, trojan, or other piece of malicious software.
		• 0x80 (bit 7) — There is a vulnerability mapped to the client detected in the event. (version 5.0+ only)
		The following impact level values map to specific priorities on the Defense Center. An x indicates the value can be 0 or 1:
		• (0, unknown): 00x00000
		• red (1, vulnerable): xxxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx (version 5.0+ only)
		• orange (2, potentially vulnerable): 00x0011x
		• yellow (3, currently not vulnerable): 00x0001x
		• blue (4, unknown target): 00x00001

Table B-8 Impact Event Data Fields (continued)

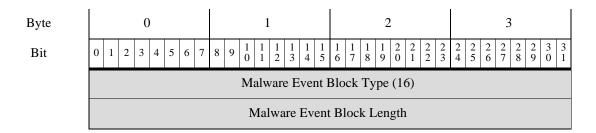
Field	Data Type	Description
Source IP Address	uint8[4]	IP address of the host associated with the impact event, in IP address octets.
Destination IP uint8[4] Address		IP address of the destination IP address associated with the impact event (if applicable), in IP address octets. This value is 0 if there 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 4-70.
String Block Length	uint32	Number of bytes in the event description string block. This includes the four bytes for the string block type, the four bytes for the string block length, and the number of bytes in the description.
Description	string	Description of the impact event.

Legacy Malware Event Data Structures

- Malware Event Data Block 5.1, page B-46
- Malware Event Data Block 5.1.1.x, page B-50
- Malware Event Data Block 5.2.x, page B-56
- Malware Event Data Block 5.3, page B-63
- Malware Event Data Block 5.3.1, page B-70
- Malware Event Data Block 5.4.x, page B-77

Malware Event Data Block 5.1

The eStreamer service uses the malware event data block to store information on malware events. These events contain information on malware detected or quarantined within a cloud, the detection method, and hosts and users affected by the malware. The malware event data block has a block type of 16 in the series 2 group of blocks. You request the event as part of the malware event record by setting the malware event flag—bit 30 in the request flags field—in the request message with an event version of 1 and an event code of 101.



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

Byte	0	1	2	3					
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 1 2 2 2 2 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 SHA Hash	String Block Type (0)								
114511		String Blo	ck Length						
		File SHA	A Hash						
		File	Size						
	File Type	File Timestamp							
Parent File Name	File Timestamp, cont.	String Block Type (0)							
	String Block Type (0), cont.	String Block Length							
	String Block Length, cont.	Parent File Name							
Parent File SHA Hash		String Bloc	k Type (0)						
Sirringsi	String Block Length								
	SHA Hash								
Event Description	String Block Type (0)								
Scottipuon		String Blo	ck Length						
	Event Description								

Table B-9 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-9 Malware Event Data Block Fields (continued)

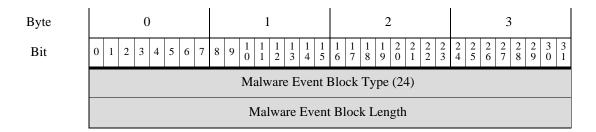
Field	Data Type	Description
Event Subtype ID	uint8	The internal ID of the action that led to malware detection.
Host IP Address	uint32	The host IP address associated with the malware event.
Detector ID	uint8	The internal ID of the detection technology that detected the malware.
String Block Type	uint32	Initiates a String data block containing the detection name. This value is always 0.
String Block Length	uint32	The number of bytes included in the Detection Name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Detection Name field.
Detection Name	string	The name of the detected or quarantined malware.
String Block Type	uint32	Initiates a String data block containing the username. This value is always 0.
String Block Length	uint32	The number of bytes included in the User String data block, including eight bytes for the block type and header fields plus the number of bytes in the User field.
User	string	The user of the computer where the Cisco Agent is installed and where the malware event occurred. Note that these users are not tied to user discovery.
String Block Type	uint32	Initiates a String data block containing the file name. This value is always o.
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-9	Mahwara	Event Data	Block	Fielde	(continued)
i apie b-9	iviaiware	Event Data	i Diock	rieias	(continuea)

Field	Data Type	Description
String Block Type	uint32	Initiates a String data block containing the parent file name. This value is always 0.
String Block Length	uint32	The number of bytes included in the Parent File Name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Parent File Name field.
Parent File Name	string	The name of the file accessing the detected or quarantined file when detection occurred.
String Block Type	uint32	Initiates a String data block containing the parent file SHA hash. This value is always 0.
String Block Length	uint32	The number of bytes included in the Parent File SHA Hash String data block, including eight bytes for the block type and header fields plus the number of bytes in the Parent File SHA Hash field.
Parent File SHA Hash	string	The SHA-256 hash value of the parent file accessing the detected or quarantined file when detection occurred.
String Block Type	uint32	Initiates a String data block containing the event description. This value is always 0.
String Block Length	uint32	The number of bytes included in the Event Description String data block, including eight bytes for the block type and header fields plus the number of bytes in the Event Description field.
Event Description	string	The additional event information associated with the event type.

Malware Event Data Block 5.1.1.x

The eStreamer service uses the malware event data block to store information on malware events. These events contain information on malware detected or quarantined within a cloud, the detection method, and hosts and users affected by the malware. The malware event data block has a block type of 24 in the series 2 group of blocks. You request the event as part of the malware event record by setting the malware event flag—bit 30 in the request flags field—in the request message with an event version of 2 and an event code of 101.



Byte	0	1	2	3
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 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 UUID), 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 7	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 Blo	ck Length	
	File Name			
File Path		String Bloc	k Type (0)	
	String Block 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 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 0
File SHA	String Block Type (0)		
Hash		String Blo	ck Length
		File SHA	A Hash
	File Size		
	File Type		File Timestamp
Parent File Name	File Timestamp, cont.		String Block Type (0)
	String Block Type (0), cont.		String Block Length
	String Block Length, cont.		Parent File Name
Parent File SHA Hash		String Bloc	k Type (0)
SIIIIII		String Blo	ck Length
	Parent File SHA Hash		
Event Description	String Block Type (0)		
		String Blo	ck Length
		Event Des	cription
		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-10 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-10 Malware Event Data Block for 5.1.1.x Fields (continued)

Field	Data Type	Description
String Block Length	uint32	The number of bytes included in the Detection Name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Detection Name field.
Detection Name	string	The name of the detected or quarantined malware.
String Block Type	uint32	Initiates a String data block containing the username. This value is always 0.
String Block Length	uint32	The number of bytes included in the User String data block, including eight bytes for the block type and header fields plus the number of bytes in the User field.
User	string	The user of the computer where the Cisco Agent is installed and where the malware event occurred. Note that these users are not tied to user discovery.
String Block Type	uint32	Initiates a String data block containing the file name. This value is always 0.
String Block Length	uint32	The number of bytes included in the File Name String data block, including eight bytes for the block type and header fields plus the number of bytes in the File Name field.
File Name	string	The name of the detected or quarantined file.
String Block Type	uint32	Initiates a String data block containing the file path. This value is always 0.
String Block Length	uint32	The number of bytes included in the File Path String data block, including eight bytes for the block type and header fields plus the number of bytes in the File Path field.
File Path	string	The file path, not including the file name, of the detected or quarantined file.
String Block Type	uint32	Initiates a String data block containing the file SHA hash. This value is always 0.
String Block Length	uint32	The number of bytes included in the File SHA Hash String data block, including eight bytes for the block type and header fields plus the number of bytes in the File SHA Hash field.
File SHA Hash	string	The rendered string of the SHA-256 hash value of the detected or quarantined file.
File Size	uint32	The size in bytes of the detected or quarantined file.
File Type	uint8	The file type of the detected or quarantined file.
File Timestamp	uint32	UNIX timestamp (seconds since 01/01/1970) of the creation of the detected or quarantined file.
String Block Type	uint32	Initiates a String data block containing the parent file name. This value is always 0.

Table B-10 Malware Event Data Block for 5.1.1.x Fields (continued)

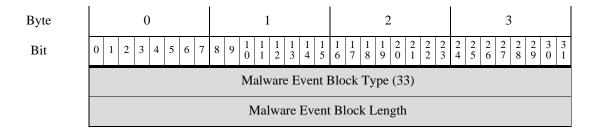
Field	Data Type	Description	
String Block Length	uint32	The number of bytes included in the Parent File Name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Parent File Name field.	
Parent File Name	string	The name of the file accessing the 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-10 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 Block Type (0)		
	String Block Type (0), cont.		String Block Length		
	String Block	String Block Length, cont. Detection Name			
User		String Bloc			
		String Bloo			
Ell M		Use			
File Name		String Bloc			
		String Bloo File Na			
File Path					
The Tath		String Block Type (0)			
	String Block Length File Path				
File SHA		String Bloc			
Hash		String Bloo			
		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 Type							
	File Timestamp								
Parent File Name	String Block Type (0)								
Trume	String Block Length								
	Parent File Name								
Parent File SHA Hash	String Block Type (0)								
SILLITUSII		String Blo	ock Length						
		Parent File SHA Hash							
Event Description		String Block Type (0)							
		String Block Length							
	Event Description								
		Devi	ice ID						
	Connection	n Instance	Connection Counter						
		Connection Ev	vent Timestamp						
	Direction		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						
			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 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, contin	nued	URI						
	Source	e Port	Destinat	ion Port						
	Source (Country	Destinatio	n Country						
		Web Appl	ication ID							
		Client App	lication ID							
	Action	Protocol								

Table B-11 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 0.

Table B-11 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 o.	
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 nat This value is always 0.			

Table B-11 Malware Event Data Block for 5.2.x Fields (continued)

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

Table B-11 Malware Event Data Block for 5.2.x Fields (continued)

Field	Data Type	Description
Access Control Policy UUID	uint8[16]	Identification number that acts as a unique identifier for the access control policy that triggered the event.
Disposition	uint8	The malware status of the file. Possible values include:
		• 1 — CLEAN — The file is clean and does not contain malware.
		• 2 — NEUTRAL — It is unknown whether the file contains malware.
		• 3 — MALWARE — The file contains malware.
		• 4 — CACHE_MISS — The software was unable to send a request to the Cisco cloud for a disposition, or the Cisco cloud services did not respond to the request.
Retrospective Disposition	uint8	Disposition of the file if the disposition is updated. If the disposition is not updated, this field contains the same value as the Disposition field. The possible values are the same as the Disposition field.
String Block Type	uint32	Initiates a String data block containing the URI. This value is always 0.
String Block Length	uint32	The number of bytes included in the URI data block, including eight bytes for the block type and header fields plus the number of bytes in the URI field.
URI	string	URI of the connection.
Source Port	uint16	Port number for the source of the connection.
Destination Port	uint16	Port number for the destination of the connection.
Source Country	uint16	Code for the country of the source host.
Destination Country	uint 16	Code for the country of the destination host.
Web Application ID	uint32	The internal identification number of the detected web application, if applicable.
Client Application ID	uint32	The internal identification number of the detected client application, if applicable.

Table B-11 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	0 1 2 3																										
Bit	0	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									3 3 0 1																
		Malware Event Block Type (35)																									
											N	Ial	wa	ıre	Ev	ent	Bl	oc.	k L	en	gth	1					
														A	λge	ent	UU	ID)								
												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 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1						
	Cloud UUID, continued									
	Cloud UUID, continued									
		Malware Eve	ent Timestamp							
		Event 7	Гуре ID							
		Event Su	ibtype 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 Blo	ck Type (0)							
		String Blo	ock Length							
		Us	er							
File Name		String Blo	ck Type (0)							
		String Blo	ock Length							
		File N	Jame							
File Path		String Blo	ck Type (0)							
		String Blo	ock Length							
		File 1	Path							
File SHA Hash		String Blo	ck Type (0)							
		String Blo	ock Length							
		File SH.	A Hash							
		File	Size							
		File	Туре							
		File Tir	mestamp							

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 Block Length								
	Parent File Name								
Parent File SHA Hash		String Block Type (0)							
		String Blo	ock Length						
		Parent File	SHA Hash						
Event Description		String Bloo	ck Type (0)						
2 computer		String Blo	ock Length						
		Event Description							
	Device ID								
	Connectio	n Instance	Connecti	on Counter					
		Connection Ev	ent Timestamp						
	Direction		Source IP Address						
		Source IP Add	ress, continued						
		Source IP Add	ress, continued						
		Source IP Add	ress, continued						
	Source IP, cont.		Destination IP Addres	s					
		Destination IP A	ddress, continued						
		Destination IP A	ddress, continued						
		Destination IP A	ddress, continued						
	Destination IP, cont		Application ID						
	App. ID, cont.		User ID						
	User ID, cont.	Ac	cess Control Policy U	UID					

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

Table B-12 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-12 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 the event. See AMP for Endpoints File Type Metadata, page 3-39 for more information.					
File Timestamp	uint32	UNIX timestamp (seconds since 01/01/1970) of the creation of the detected or quarantined file.					

Table B-12 Malware Event Data Block for 5.3 Fields (continued)

Field	Data Type	Description								
String Block Type	uint32	Initiates a String data block containing the parent file name. This value is always 0.								
String Block Length	uint32	The number of bytes included in the Parent File Name String data block, including eight bytes for the block type and header fields plus the number of bytes in the Parent File Name field.								
Parent File Name	string	The name of the file accessing the detected or quarantined file when detection occurred.								
String Block Type	uint32	Initiates a String data block containing the parent file SHA hash. This value is always 0.								
String Block Length	uint32	The number of bytes included in the Parent File SHA Hash String data block, including eight bytes for the block type and header fields plus the number of bytes in the Parent File SHA Hash field.								
Parent File SHA Hash	string	The SHA-256 hash value of the parent file accessing the detected or quarantined file when detection occurred.								
String Block Type	uint32	Initiates a String data block containing the event description. This value is always 0.								
String Block Length	uint32	The number of bytes included in the Event Description String data block, including eight bytes for the block type and header fields plus the number of bytes in the Event Description field.								
Event Description	string	The additional event information associated with the event type.								
Device ID	uint32	ID for the device that generated the event.								
Connection Instance	uint16	Snort instance on the device that generated the event. Used to link the event with a connection or IDS event.								
Connection Counter	uint16	Value used to distinguish between connection events that happen during the same second.								
Connection Event Timestamp	uint32	Timestamp of the connection event.								
Direction	uint8	Indicates whether the file was uploaded or downloaded. Can have the following values: • 1 — Download • 2 — Upload								
		Currently the value depends on the protocol (for example, if 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-12 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.						
		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 clapplication, if applicable.								

Table B-12 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 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	2 7	2 8	2 9	3	3
	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 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1								
	Cloud UUID											
	Cloud UUID, continued											
	Cloud UUID, continued											
	Cloud UUID, continued											
	Malware Event Timestamp											
	Event Type ID											
		Event Su	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	ck Type (0)									
	String Block Length											
		Use	er									
File Name		String Bloc	ck Type (0)									
		String Blo	ck Length									
		File N	ame									
File Path		String Bloc	ck Type (0)									
		String Blo	ck Length									
		File F	Path									
File SHA Hash		String Bloo	ck Type (0)									
	String Block Length											
		File SHA	A Hash									
	File Size											
		File '										
	File Timestamp											

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								
Parent File		String Bloo	ck Type (0)									
Name	String Block Length											
		Parent Fi	le Name									
Parent File SHA Hash	String Block Type (0)											
SHA Hash		String Blo	ock Length									
	Parent File SHA Hash											
Event Description	String Block Type (0)											
Bescription		String Block Length										
	Event Description											
	Device ID											
	Connection Instance Connection Counter											
		Connection Ev	ent Timestamp									
	Direction		Source IP Address									
		Source IP Add	ress, continued									
		Source IP Add	ress, continued									
		Source IP Add	ress, continued									
	Source IP, cont.		Destination IP Addres	s								
		Destination IP A	ddress, continued									
	Destination IP Address, continued Destination IP Address, continued Destination IP, cont Application ID											
	App. ID, cont.		User ID									
	User ID, cont.	Ac	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 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 Policy UUID, continued										
		Access Control Police	cy UUID, continued								
	Access Control Policy UUID, continued										
URI	AC Pol UUID, cont.	Disposition	Retro. Disposition	Str. Block Type (0)							
	String	String Block Length									
	Strin	g Block Length, contin	nued	URI							
	Source	e Port	Destinat	ion Port							
	Source (Country	Destination	n Country							
		Web Appl	ication ID								
		Client App	lication ID								
	Action	Protocol	Threat Score	IOC Number							
	IOC Number, cont.		Security Context								
	Security Context, continued										
	Security Context, continued										
	Security Context, continued										
	Security Cont., cont.										

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

Table B-13 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-13 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-13 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 3-39 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 Strin 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-13 Malware Event Data Block for 5.3.1 Fields (continued)

Field	Data Type	Description
Direction	uint8	Indicates whether the file was uploaded or downloaded. Can have the following values:
		• 1 — Download
		• 2 — Upload
		Currently the value depends on the protocol (for example, if the connection is HTTP it is a download).
Source IP Address	uint8[16]	IPv4 or IPv6 address for the source of the connection.
Destination IP Address	uint8[16]	IPv4 or IPv6 address for the destination of the connection.
Application ID	uint32	ID number that maps to the application using the file transfer.
User ID	uint32	Identification number for the user logged into the destination host, as identified by the system.
Access Control Policy UUID	uint8[16]	Identification number that acts as a unique identifier for the access control policy that triggered the event.
Disposition	uint8	The malware status of the file. Possible values include:
		• 1 — CLEAN The file is clean and does not contain malware.
		• 2 — UNKNOWN It is unknown whether the file contains malware.
		• 3 — MALWARE The file contains malware.
		 4 — UNAVAILABLE The software was unable to send a request to the Cisco cloud for a disposition, or the Cisco cloud services did not respond to the request.
		• 5 — CUSTOM SIGNATURE The file matches a user-defined hash, and is treated in a fashion designated by the user.
Retrospective Disposition	uint8	Disposition of the file if the disposition is updated. If the disposition is not updated, this field contains the same value as the Disposition field. The possible values are the same as the Disposition field.
String Block Type	uint32	Initiates a String data block containing the URI. This value is always 0.
String Block Length	uint32	The number of bytes included in the URI data block, including eight bytes for the block type and header fields plus the number of bytes in the URI field.
URI	string	URI of the connection.
Source Port	uint16	Port number for the source of the connection.
Destination Port	uint16	Port number for the destination of the connection.
Source Country	uint16	Code for the country of the source host.
Destination Country	uint 16	Code for the country of the destination host.

Table B-13 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.

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	6 7 8 9 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9										
	Malware Event Block Type (47)											
	Malware Event Block Length											
		Agent 1	UUID									
		Agent UUID), continued									
		Agent UUID), continued									
		Agent UUID), continued									
		Cloud	UUID									
		Cloud UUID), continued									
		Cloud UUID), continued									
		Cloud UUID), continued									
		Malware Even	nt Timestamp									
		Event T	Type ID									
Γ		Event Sub										
Detection Name	Detector ID		String Block Type (0)									
	String Block Type (0), cont.		String Block Length									
	String Block Length, cont.		Detection Name									
User		String Block	k Type (0)									
		String Bloo	ck Length									
	User											
File Name		String Block	k Type (0)									
		String Bloo	ck Length									
		File Na	ame									

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	3 3 0 1									
File Path	String Block Type (0)												
	String Block Length												
	File Path												
File SHA Hash	String Block Type (0)												
114011		String Blo	ock Length										
		File SH	A Hash										
		File Size											
	File Type												
		File Timestamp											
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										
	D' '	Connection Ev	vent Timestamp										
	Direction Source IP Address												
		Source IP Address, continued Source IP Address, continued											
			dress, continued										
	Source IP, cont.		Destination IP Address										

Byte		1									2							3										
Bit	0 1 2	8	9	10	1	1 2	1 3	1 4		1 6	1 7	1 1 8 9	,	2 0 1	2 2	2	2 4	2 5	2 6	2 7	2 8	2 9	3	3				
	Destination IP Address, continued																											
		Destination IP Address, continued																										
	Destination IP Address, continued																											
	Dest	Destination IP, cont Application ID																										
	App). II), c	ont.												Use	er	ID										
	Use	r IE), co	ont.								A	cce	ess	Co	ontro	ol	Pol	су	UI	UIE)						
						1	Acc	ces	ss C	Cont	rol	l Po	olic	y L	JU:	ID,	со	ntin	uec	i								
						1	Acc	ces	ss C	Cont	rol	l Po	olic	y L	JU	ID,	со	ntin	uec	l								
						1	Acc	ces	ss C	Cont	rol	l Po	olic	y L	JU	ID,	со	ntin	uec	i								
URI	AC	Pol coi		JID,]	Di	ispo	siti	on			R	etr	o. D	is	posi	tioı	n	S	tr.	Bl	ock	T	ype	(0))
				St	rinş	g B	loc	k	Тур	pe (0),	co	ntir	nue	ed							S		ing Len				
				S	trin	g I	Blo	ck	. Le	ngt	h, o	con	tin	uec	d									UR	I	,		
				So	urc	e P	ort											D	esti	na	tio	ı P	ort					
				Sour	ce (Coi	ıntı	ry]	Des	tina	atio	on Country							
										W	eb	Ap	pli	cati	ion	ID												
										Cli	ent	t A	ppl	ica	tio	n ID)											
		Act	ion					P	Prot	oco	1				T	hrea	t S	Scoi	e			I	OC	CN	um	ıbeı	r	
	IOC N	lum	ber	, con	t.									S	Sec	urity	<i>y</i> (Con	ext									
									Sec	curi	ty	Co	nte	xt,	co	ntin	ue	d										
	Security Context, continued																											
	Security Context, continued Security Cont., cont. SSL Certificate Fingerprint																											
							SS	L	Cei	rtifi	cat	te F	ing	gerp	prii	nt, c	on	tinı	ied									
							SS	L	Cei	rtifi	cat	te F	ing	gerp	prii	nt, c	on	tinu	ied									

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										
	SSL Certificate Fingerprint, continued										
	SSL Certificate 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										

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

Table B-14 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-14 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 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 3-39 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-14 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-14 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-14 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-14 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-14 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 List Unavailable' • 22 — 'Internal Certificate List Unavailable' • 23 — 'Internal Certificate List Unavailable' • 25 — 'Internal Certificate Unavailable' • 25 — 'Internal Certificate 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 o. 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 Name of the parent archive. string 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.

Table B-14 Malware Event Data Block for 5.4.x Fields (continued)

Legacy Discovery Data Structures

- Legacy Discovery Event Header, page B-88
- Legacy Server Data Blocks, page B-90
- Legacy Client Application Data Blocks, page B-91
- Legacy Scan Result Data Blocks, page B-92
- Legacy Host Profile Data Blocks, page B-115
- Legacy OS Fingerprint Data Blocks, page B-122

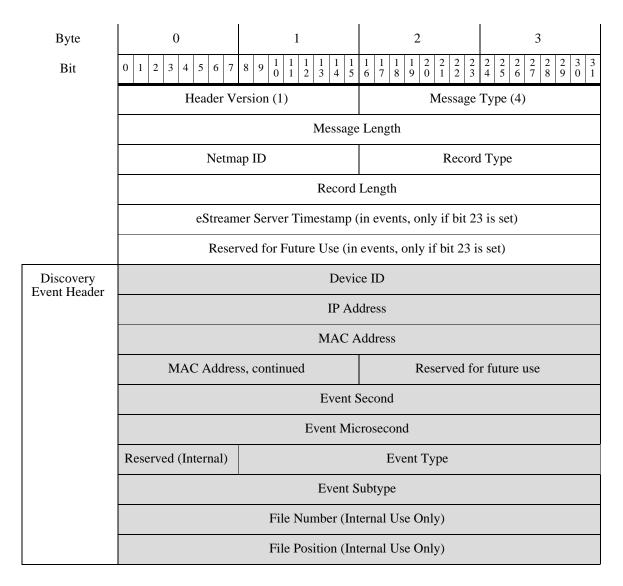
Legacy Discovery Event Header

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 4-42.

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-15 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 3-34 for more information.	
IP Address	uint32	IP address of the host involved in the event.	
MAC Address	uint8[6]	AC 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.	

Table B-15 Discovery Event Header Fields (continued)

Field	Data Types	Description
Event Microsecond	uint32	Microsecond (one millionth of a second) increment that the system generated the event.
Reserved (Internal)	byte	Internal data from Cisco and can be disregarded.
Event Type	uint32	Event type (1000 for new events, 1001 for change events, 1002 for user input events, 1050 for full host profile). See Host Discovery Structures by Event Type, page 4-42 for a list of available event types.
Event Subtype	uint32	Event subtype. See Host Discovery Structures by Event Type, page 4-42 for a list of available event subtypes.
File Number	byte[4]	Serial file number. This field is for Cisco internal use and can be disregarded.
File Position	byte[4]	Event's position in the serial file. This field is for Cisco internal use and can be disregarded.

Legacy Server Data Blocks

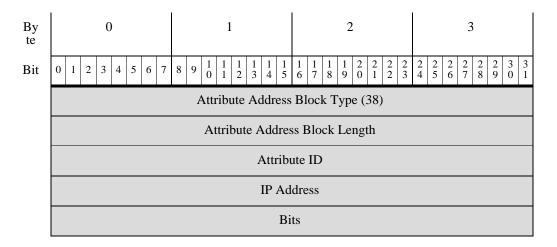
For more information, see the following sections:

• Attribute Address Data Block for 5.0 - 5.1.1.x, page B-90

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-16 Attribute Address Data Block Fields

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

Legacy Client Application Data Blocks

For more information, see the following sections:

• User Client Application Data Block for 5.0 - 5.1, page B-91

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	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 Client Application Block Type (59)				
		User Client Applica	ation 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-17 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 4-58User Server Data Block Fields, page 4-101 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-93
- User Product Data Block for 5.0.x, page B-95
- User Information Data Block for 5.x, page B-113

Scan Result Data Block 5.0 - 5.1.1.x

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

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

Byte	0 1		2	3			
Bit	0 1 2 3 4 5 6 7 8 9 1 1 1 2 3	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			
	Scan Re	Scan Result Block Type (102)					
	Scan F	Result I	Block Length				
		Use	r ID				
		Scan	Туре				
		IP Ad	ldress				
	Port		Proto	ocol			
	Flag		List Block	Type (11)	Scan Vulnerability		
	List Block Type (11)	List Block Length		List			
Vulnerability List	List Block Length Scan Vulnerability Block Type (109)						
2350	Scan Vulnerability Block Type (109) Scan Vulnerability Block Length						
	Scan Vulnerability Block Length Vulnerability Data						
	List Block Type (11)				Generic Scan Results List		
	List Block Length						
Scan Results List	Generic Scan Results Block Type (108)						
	Generic Sc						
	Generic Scan Results						
User Product List	Generic List Block Type (31)						
2 1 3 4 4 5 1 5 1	Generic List Block Length						
	User Product Data Blocks*						

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

Table B-18 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-18 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	formation 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 4-167 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-189 and User Server and Operating System Messages, page 4-55. 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 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)				
Runges	Generic List Block Length				
	IP Range Specification 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
	Po	ort	Prot	ocol
		Drop User	r Product	
Custom Vendor String		String Bloc	k Type (0)	
vendor string		String Bloo	ck Length	
		Custom Ven	dor String	
Custom Product String		String Bloc	k Type (0)	
Troduct String		String Bloo	ck Length	
		Custom Prod	uct String	
Custom Version String		String Bloc	k Type (0)	
String Block Length				
	Custom Version String			
	Software ID			
	Server ID			
	Vendor ID			
	Product ID			
Major Version String	String Block Type (0)			
		String Bloo	ck Length	
	Major Version String			
Minor Version String				
String Block Length				
	Minor Version String			
Revision String		String Bloc	k Type (0)	
		String Bloo	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 1 2 2 2 2 2		
To Major String	String Block Type (0)		
Sumg	String Block Length		
	To Major Version String		
To Minor String	String Block Type (0)		
String	String Block Length		
	To Minor Version String		
To Revision String	String Block Type (0)		
Sumg	String Block Length		
	To Revision String		
Build String	String Block Type (0)		
	String Block Length		
	Build String		
Patch String	String Block Type (0)		
	String Block Length		
	Patch String		
Extension String	String Block Type (0)		
28	String Block Length		
	Extension 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 List Block Length		
	Fix List Data Blocks*		

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

Table B-19 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 4-93 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-19 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-19 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 eigh 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 3 operating system definitions that a third party operating system stri in the user input is mapped to.	
String Block Type	uint32	Initiates a String data block containing the build number of the Cisc 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]	ontains 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 4-100 for a description of this data block.	

Table B-19 User Product Data Block Fields for 4.10.x, 5.0-5.0.x (continued)

Legacy User Login Data Blocks

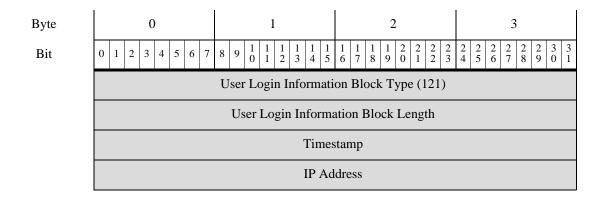
See the following sections for more information:

- User Login Information Data Block for 5.0 5.0.2, page B-101
- User Login Information Data Block 5.1-5.4.x, page B-103
- User Login Information Data Block 6.0.x, page B-105
- User Information Data Block for 5.x, page B-113

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 4-60.

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



Byte	0	0 1		3	
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 1 5	1 1 1 1 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 Name	String Block Type (0)				
Tvarre	String Block Length				
	User Name				
	User ID				
	Application ID				
Email	String Block Type (0)				
	String Block Length				
	Email				

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

Table B-20 User Login Information Data Block Fields 5.0 - 5.0.2

Field	Data Type	Description	
User Login Information Block Type	uint32	Initiates a User Login Information data block. This value is 121 for version 5.0 - 5.0.2.	
User Login Information Block Length	uint32	Total number of bytes in the User Login Information data block, including eight bytes for the user login information block type and length fields, plus the number of bytes in the user login information data that follows.	
Timestamp	uint32	Timestamp of the event.	
IP Address	uint8[4]	IP address from the host where the user was detected logging in, in IP address octets.	
String Block Type	uint32	Initiates a String data block containing the username for the user. This value is always 0.	
String Block Length	uint32	Number of bytes in the username String data block, including eight bytes for the block type and length fields, plus the number of bytes in the username.	
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-20 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 4-175.

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 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 Address											
User Name		String Block Type (0)										
Tvarice		String Blo	ck Length									
		User N	lame									
		User	r ID									
		Applica	tion ID									
Email		String Bloc	k Type (0)									
		String Blo	ck Length									
		Email										
		IPv6 Address										
	IPv6 Address, continued											
		IPv6 Addres	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 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	String Block Type (0)												
	String Block Type (0), cont.	String Block Length												
	String Block Length	Reported By												

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

Table B-21 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 1-5 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.

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 4-175.

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-103 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 1 1 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0												
	User Login Infor	User Login Information Block Type (159)											
	User Login Information Block Length												
	Timestamp												
	IPv4 Address												
User Name	String	Block Type (0)											
Tame	String	String Block Length											
	Us	User Name											
Domain	String	String Block Type (0)											
	String Block Length												
	Domain												
	User ID												

Byte	0							1								2									3											
Bit	0 1	2	2 3	3 4	5	6	7	8	9	(1	1 1	1 2	1	1 4		1 5	1 6	1 7		1 3	2	2	2	2 2	2 3	2	2	2 5	2 6	2 7	2 8	2 9	3	3	3
		Realm ID																																		
		Endpoint Profile ID																																		
		Security Group ID																																		
														A	App	lic	cat	tio	n I	D	1															
															F	rc	otc	cc	ol																	
Email		String Block Type (0)																																		
		String Block Length																																		
	Email																																			
		IPv6 Address																																		
		IPv6 Address, continued																																		
												I	Pve	5 4	Ado	lre	ess	5, 0	cor	ıti	nu	ed														
												Il	Pve	5 4	Ado	lre	ess	5, 0	or	ıti	nu	ed														
]	Loc	ca	tioı	ı I	Pv	v6	A	dc	lres	S														
]	L	oca	ati	ion	Ι	Pve	5 A	Αd	dr	ess	ς,	cor	tin	ue	ed												
]	L	oca	ati	ion	Ι	Pve	i A	Αd	dr	ess	3,	cor	tin	u	ed												
]	L	oca	ati	ion	Ι	Pv6	5 A	٩d	dr	ess	ς,	cor	tin	u	ed												
Reported By		Lo	ogiı	n T	ype					A	utl	h.	Ту	p	e							S	tri	ng	В	lo	ck	T	уp	e ((0)					
			St	ring	g Bl	ocl	k T	ур	e ((0)), (СО	nt.									Ş	String Block Length													
			S	trin	String Block Length, cont. Reported By																															

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

Table B-22 User Login Information Data Block Fields

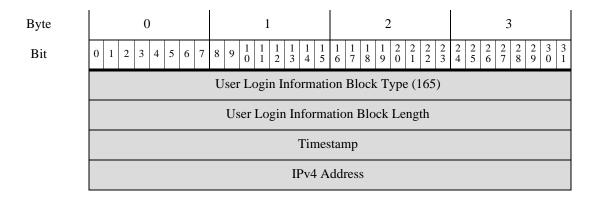
Field	Data Type	Description
User Login Information Block Type	uint32	Initiates a User Login Information data block. This value is 159 for version 6.0.x.
User Login Information Block Length	uint32	Total number of bytes in the User Login Information data block, including eight bytes for the user login 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.
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 1-5 for more information.
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.
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.
Application ID	uint32	The application ID for the application protocol used in the connection that the login information was derived from.
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

Table B-22 User Login Information Data Block Fields (continued)

Field	Data Type	Description
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: o - no authorization required 1 - passive authentication, AD agent, or ISE session c - captive portal successful authentication a - 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-105 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 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
User Name		String Bloo	ck Type (0)	
Name		String Blo	ock Length	
		User N	Name	
Domain		String Bloo	ck Type (0)	
		String Blo	ock Length	
		Dom	ain	
		Use	r ID	
		Real	m ID	
		Endpoint	Profile ID	
		Security	Group ID	
		Applica	ation ID	
	Protocol			
	Po	ort	Range Start	
	Start	t Port	End Port	
Email		String Bloc	ck Type (0)	
		String Blo	ock Length	
		Ema	ail	
		IPv6 A	Address	
		IPv6 Addres	ss, continued	
		IPv6 Addres	ss, continued	
	IPv6 Address, continued Location IPv6 Address			
		Location IPv6 A	ddress, continued	
		Location IPv6 A	ddress, continued	
		Location IPv6 Ac	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 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1	
Reported By	Login Type	Auth. Type	String Block Type (0)		
	String Block Type (0), cont.		String Blo	ck Length	
	String Block Length, cont.		Reporte	ed By	

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

Table B-23 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 1-5 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.
Application ID	uint32	The application ID for the application protocol used in the connection that the login information was derived from.

Table B-23 User Login Information Data Block Fields (continued)

Field	Data Type	Description
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:
		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 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 4-59

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	0	1	2	3	
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 3 3 4 5 6 7 8 9 0 1	
		User Information Blo	ock Type (75 120)		
		User Information Block Length			
		User	·ID		
User Name		String Block	k Type (0)		
rvanic		String Bloo	ck Length		
		User N	ame		
		Proto	ocol		
First Name	String Block Type (0)				
Tunie	String Block Length				
		First N	ame		
Last String Block Type (0) Name					
Tunie	String Block Length				
		Last Na	ame		
Email	String Block Type (0)				
	String Block Length				
		Ema	il		
Department		String Block	k Type (0)		
		String Bloo	ck Length		
		Departr	ment		

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	
Phone	String Block Type (0)	
	String Block Length	
	Phone	

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

Table B-24 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 0.	
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.	
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 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.	

Field Data Type Description Email The email address for the user. string String Block Type uint32 Initiates a String data block containing the department for the user. This value is always o. 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.

The phone number for the user.

Table B-24 User Information Data Block Fields (continued)

Legacy Host Profile Data Blocks

Phone

See the following sections for more information:

string

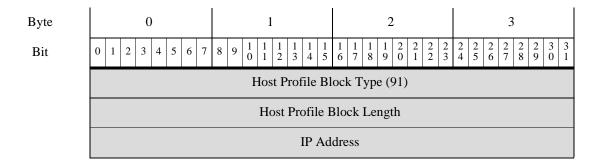
• Host Profile Data Block for 5.0 - 5.0.2, page B-115

Host Profile Data Block for 5.0 - 5.0.2

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



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



Byte	0	1	2	3	
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1	
Server Fingerprints	Hops	Primary/Secondary	Generic List B	lock Type (31)	
Tingerprints	Generic List Block	Type, continued	Generic List 1	Block Length	
	Generic List Block	Length, continued	Server Fingerpri	nt Data Blocks*	
Client Fingerprints		Generic List Bl	lock Type (31)		
1 mgcrprmts		Generic List I	Block Length		
		Client Fingerprin	nt Data Blocks*		
SMB Fingerprints		Generic List Bl	lock Type (31)		
ingerprines		Generic List I	Block Length		
		SMB Fingerprin	nt Data Blocks*		
DHCP Fingerprints	Generic List Block Type (31)				
g	Generic List Block Length				
	DHCP Fingerprint Data Blocks*				
	List Block Type (11)			List of TCP Servers	
	List Block Length				
TCP Server Block*	Server Block Type (36)				
	Server Block Length				
	TCP Server Data				
	List Block Type (11)			List of UDP Servers	
	List Block Length				
UDP Server Block*		Server Block	Type (36)*		
	Server Block Length				
		UDP Serv	er Data		

Byte	0	1 2	3		
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1		
		List Block Type (11)		List of Network	
		List Block Length		Protocols	
Network Protocol		Protocol Block Type (4)*			
Block*		Protocol Block Length			
		Network Protocol Data			
		List Block Type (11)		List of Transport	
		List Block Length		Protocols	
Transport Protocol		Protocol Block Type (4)*			
Block*		Protocol Block Length			
		Transport Protocol Data			
			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	VLAN ID	VLAN Type		
	VLAN Priority	Generic List Block Type (31)	List of Client Applications	
	Generic List Block Type, continued	Generic List Block Leng	th		
Client App Data	Generic List Block Length, continued	Client Application Block Type	(112)*		
	Client App Block Type (29)*, con't	Client Application Block Le	ength		
	Client Application Block Length, con't	Client Application Data.			

Byte	0 1 2 3		
Bit	0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2		
NetBIOS Name	String Block Type (0)		
Tame	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-25 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-122 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-25 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-122 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-122 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-122 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-25 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 4-74.
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 4-74.
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-25 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 4-113.
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 — Bridge3 — 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 4-152.
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-25 Host Profile Data Block for 5.0 - 5.0.2 Fields (continued)

Field	Data Type	Description
String Block Length		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-122

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	3												
Bit		3												
	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-26 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-124
- Connection Statistics Data Block 5.1, page B-128
- Connection Statistics Data Block 5.2.x, page B-134
- Connection Chunk Data Block for 5.0 5.1, page B-140
- Connection Chunk Data Block for 5.1.1-6.0.x, page B-141
- Connection Statistics Data Block 5.1.1.x, page B-143
- Connection Statistics Data Block 5.3, page B-149
- Connection Statistics Data Block 5.3.1, page B-156
- Connection Statistics Data Block 5.4, page B-163
- Connection Statistics Data Block 5.4.1, page B-176
- Connection Statistics Data Block 6.0.x, page B-189

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 4-51.

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 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 Data 1	Block Type (115)												
		Connection Data	a Block Length												
		Devic	ce ID												
		Ingress	s Zone												
	Ingress Zone, continued														
	Ingress Zone, continued														
	Ingress Zone, continued														
	Egress Zone														
		Egress Zone	e, continued												
		Egress Zone	e, continued												
		Egress Zone	e, continued												
		Ingress I	nterface												
		Ingress Interfa	ice, continued												
		Ingress Interfa	ice, continued												
		Ingress Interfa	ice, continued												
		Egress In	nterface												
		Egress Interfa	ce, continued												
		Egress Interfa	ce, continued												
		Egress Interfa	ce, continued												
		Initiator II	P Address												
		Initiator IP Add	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 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 Add	ress, continued												
		Initiator IP Add	ress, continued												
		Responder	IP Address												
		Responder IP Ad	ldress, continued												
		Responder IP Ad	ldress, continued												
		Responder IP Ad	ldress, continued												
	Policy Revision														
	Policy Revision, continued														
	Policy Revision, continued														
	Policy Revision, continued														
	Rule ID														
		Rule A	Action												
	Initiato	or Port	Respon	der Port											
	TCP I	Flags	Protocol	NetFlow Source											
		NetFlow Sour	ce, continued												
		NetFlow Sour	ce, continued												
		NetFlow Sour													
		tFlow Source, continue		First Pkt Time											
		acket Timestamp, cont		Last Pkt Time											
	Last Pa	acket Timestamp, cont		Packets Sent											
		Packets Sen													
	P	Packets Sent, continued		Packets Rcvd											
	_	Packets Receiv													
	Pac	kets Received, continu		Bytes Sent											
	T)	Bytes Sent,		Dates D. 1											
	Pac	kets Received, continu	iea	Bytes Rcvd											

Byte	0	0 1 2										
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 3 3 3 4 5 6 7 8 9 0 1								
	В	User ID										
		User ID, continued		Application Protocol ID								
	Applio	cation Protocol ID, cont	tinued	URL Category								
	U	JRL Category, continue	d	URL Reputation								
	UI	RL Reputation, continu	ed	Client App ID								
	Clier	nt Application ID, conti	nued	Web App ID								
	Web	Application ID, contin	nued	String Block Type (0)								
Client App URL	Stri	ing Block Type, continu	ued	String Block Length								
	Strir	ng Block Length, contin	nued	Client Application URL								
NetBIOS Name		String Bloc	k Type (0)									
Tunie		String Blo	ck Length									
		NetBIOS	Name									
Client App Version		String Bloc	k Type (0)									
pp , staton		String Bloo	ck Length									
		Client Applica	tion Version									

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

Table B-27 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.

Table B-27 Connection Statistics Data Block 5.0 - 5.0.2 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	uint32	The action selected in the user interface for that rule (allow, block, and so forth).
Initiator Port	uint16	Port used by the initiating host.
Responder Port	uint16	Port used by the responding host.
TCP Flags	uint16	Indicates any TCP flags for the connection event.
Protocol	uint8	The IANA-specified protocol number.
NetFlow Source	uint8[16]	IP address of the NetFlow-enabled device that exported the data for the connection
First Packet Timestamp	uint32	UNIX timestamp of the date and time the first packet was exchanged in the session.
Last Packet Timestamp	uint32	UNIX timestamp of the date and time the last packet was exchanged in the session.
Packets Sent	uint64	Number of packets transmitted by the initiating host.
Packets Received	uint64	Number of packets transmitted by the responding host.
Bytes Sent	uint64	Number of bytes transmitted by the initiating host.
Bytes Received	uint64	Number of bytes transmitted by the responding host.
User ID	uint32	Internal identification number for the user who last logged into the host that generated the traffic.
Application Protocol ID	uint32	Application ID of the application protocol.
URL Category	uint32	The internal identification number of the URL category.
URL Reputation	uint32	The internal identification number for the URL reputation.
Client Application ID	uint32	The internal identification number of the detected client application, if applicable.
Web Application ID	uint32	The internal identification number of the detected web application, if applicable.
String Block Type	uint32	Initiates a String data block for the client application URL. This value is always 0.

Table B-27 Connection Statistics Data Block 5.0 - 5.0.2 Fields (continued)

Field	Data Type	Description
String Block Length	uint32	Number of bytes in the client application URL String data block, including eight bytes for the string block type and length fields, plus the number of bytes in the 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 4-51.

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	8	9	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
	Connection Data Block Type (126)																															
	Connection Data Block Length																															
	Device ID																															
														Iı	ngr	ess	Zo	one	,													
												Iı	ngı	ess	Σ	one	e, c	on	tinı	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 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			
		Ingress Zone, continued					
		Ingress Zone, continued					
		Egress	Zone				
		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 In	nterface				
		Egress Interfa	ce, continued				
		Egress Interfa	ce, continued				
		Egress Interfa	ce, continued				
		Initiator II	Address Address				
		Initiator IP Add	ress, continued				
		Initiator IP Add					
		Initiator IP Add					
		Responder					
		Responder IP Ad					
		Responder IP Ad					
		Responder IP Address, continued					
		Policy Revision					
		Policy Revision					
		Policy Revision					
		Policy Revision	on, continued				

Byte				0								1								2					3							
Bit	0 1	2	2 3	3 4	4	5 6	7	8	ç	$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$		1 2	1 3	l 3	1 1 4 5	1 6		1 1 7 8		1 9	20	2	2 2	2 3	2 4	2 5	2	2 7	2 8	2	3	3
		Rule ID																														
						Ru	le A	Αc	tio	n												F	Rul	e I	Rea	son						
						Ini	tiato	or	Po	rt												Re	esp	on	der	Por	t					
						T	CP :	Fla	ags	S								I	Pro	otc	со	l				Net	Flo	эw	So	ur	ce	
											1	Netl	Flo	W	Sou	rce,	, (cont	tir	ıue	ed											
											ľ	Netl	Flo	W	Sou	rce,	, (con	tir	ıue	d											
											ľ	Netl	Flo	W	Sou	rce,	, (con	tir	ıue	d											
							Ne	etF	lo	w S	o	urc	e, c	OI	ntinu	ed										Fir	st	Pk	t Ti	m	e	
						Fir	st F	ac	ke	t Ti	in	nest	am	ıp.	, con	tinı	ue	ed								La	st	Pk	t Ti	m	e	
		Last Packet Timestamp, continued Initiator Transmitted Packets																														
		Initiator Transmitted Packets, continued																														
	Initiator Transmitted Packets, continued Responder Transmitted Packets																															
		Responder Transmitted Packets, continued																														
				R	les	spoi	nde	r T	ra	nsn	ni	ttec	l Pa	acl	kets,	COI	nt	inu	ec	i					7	Γran			ator ed l		tes	S
									Iı	nitia	at	or T	[ra	ns	mitte	ed I	By	ytes	, (coı	ntir	ıue	ed									
					I	niti	ator	·T	raı	nsm	it	tted	Ву	∕t€	es, co	nti	n	ued] 7	F ran	Res sm	spo nitt	nde ed]	er By	tes	S
									Re	spo	n	der	Tr	an	smit	ted	F	3yte	es,	, co	ont	inı	ued	l								
]	Re	espo	onde	er	Tr	ansı	m	itte	d F	Зу	tes,	con	ti	nue	d								U	ser	ID			
	User ID, continued Application Protocol ID																															
		Application Protocol ID, continued				ed								UF	L	Ca	iteg	or	у													
							U	R]	L (Cate	g	ory	, c	on	tinu	ed										UR	LI	Rep	outa	itio	on	
							UF	RL	R	epu	ta	atio	n, c	co	ntinı	ed										Cli	en	ıt A	App	II)	
						C	lien	t 1	Aр	plic	a	tior	ı II),	cont	inu	ec	1								W	eb	A	pp	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		
	Web	Web Application ID, continued String Block Type (0)				
Client App URL	Stri	String Block Type, continued String Block Length				
	Strin	String Block Length, continued Client Application URL				
NetBIOS Name		String Bloc	k Type (0)			
Tume		String Blo	ck Length			
		NetBIOS	Name			
Client App Version		String Block Type (0)				
Tipp (Closest		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. Rep Layer				

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

Table B-28 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.

Table B-28 Connection Statistics Data Block 5.1 Fields (continued)

Field	Data Type	Description
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.
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.

Table B-28 Connection Statistics Data Block 5.1 Fields (continued)

Field	Data Type	Description
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.
Monitor Rule 8	uint32	The ID of the eighth monitor rule associated with the connection event.

Table B-28 Connection Statistics Data Block 5.1 Fields (continued)

Field	Data Type	Description
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-143.

For more information on the Connection Statistics Data message, see Connection Statistics Data Message, page 4-51.

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 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 (144)				
		Connection Data Block Length					
		Devic	e ID				
		Ingress	Zone				
		Ingress Zone, continued					
	Ingress Zone, continued						
		Ingress Zone, continued					
		Egress	Zone				
		Egress Zone	, continued				
		Egress Zone, continued					
	Egress Zone, continued						
		Ingress I	nterface				
		Ingress Interfa	ce, continued				

Byte	0	1	2	3		
Bit	0 1 2 3 4 5 6 7 8	3 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		
	Ingress Interface, continued					
		Ingress Interfa	ace, continued			
		Egress I	nterface			
		Egress Interfa	ce, continued			
		Egress Interfa	ce, continued			
		Egress Interfa	ce, continued			
		Initiator II	P Address			
		Initiator IP Add	ress, continued			
		Initiator IP Add	ress, continued			
		Initiator IP Add	ress, continued			
	Responder IP Address					
	Responder IP Address, continued					
	Responder IP Address, continued					
	Responder IP Address, continued					
		Policy R				
		Policy Revision				
		Policy Revision				
		Policy Revision				
	D 1 4	Rule				
	Rule Ac		Rule R			
	Initiator		Respond			
	TCP FI		Protocol	NetFlow Source		
		NetFlow Sour				
		NetFlow Sour				
	NIA	NetFlow Source continu		Instance ID		
	Neti	Flow Source, continu	eu	mstance 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 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			
	Instance ID, cont.	Connection	n Counter	First Pkt Time			
	First P	First Packet Timestamp, continued					
	Last P	Last Packet Timestamp, continued Initiator Packets					
		Initiator Transmitted Packets, continued					
	Initiator '	Initiator Transmitted Packets, continued Resp. Tx Packets					
		Responder Transmitte	ed Packets, continued				
	Responder	r Transmitted Packets,	continued	Initiator Tx Bytes			
		Initiator Transmitte	d Bytes, continued				
	Initiator	Transmitted Bytes, co	ntinued	Resp. Tx Bytes			
		Responder Transmitt	ed Bytes, continued				
	Responder Transmitted Bytes, continued User ID						
		User ID, continued		Application Prot. ID			
	Applic	eation Protocol ID, cont	tinued	URL Category			
	U	RL Category, continue	d	URL Reputation			
	UF	RL Reputation, continue	ed	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, contin	nued	Client App. URL			
NetBIOS Name		String Bloc	k Type (0)				
Traine		String Bloo	ck Length				
		NetBIOS	Name				
Client App Version		String Bloc	k Type (0)				
		String Bloo	ck Length				
		Client Applicat	tion Version				

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 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 Even	nt Count				
Intrusion E	Intrusion Event Count Initiator Country						
Responder							

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

Table B-29 Connection Statistics Data Block 5.2.x Fields

Field	Data Type	Description
Connection Statistics Data Block Type	uint32	Initiates a Connection Statistics data block for 5.2.x. The value is always 144.
Connection Statistics Data Block Length	uint32	Number of bytes in the Connection Statistics data block, including eight bytes for the connection statistics block type and length fields, plus the number of bytes in the connection data that follows.
Device ID	uint32	The device that detected the connection event.
Ingress Zone	uint8[16]	Ingress security zone in the event that triggered the policy violation.
Egress Zone	uint8[16]	Egress security zone in the event that triggered the policy violation.
Ingress Interface	uint8[16]	Interface for the inbound traffic.
Egress Interface	uint8[16]	Interface for the outbound traffic.
Initiator IP Address	uint8[16]	IP address of the host that initiated the session described in the connection event, in IP address octets.
Responder IP Address	uint8[16]	IP address of the host that responded to the initiating host, in IP address octets.

Table B-29 Connection Statistics Data Block 5.2.x Fields (continued)

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

Table B-29 Connection Statistics Data Block 5.2.x Fields (continued)

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

Table B-29 Connection Statistics Data Block 5.2.x Fields (continued)

Field	Data Type	Description
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 2	1 3	1 4	1 5	1 6	1 7		1 9	2 0	2	2 2	2 3	2 4	2 5	2 6	2 7	2 8	2 9	3 0 1	1					
									C	on	nec	ctic	n (Ch	unk	В.	loc	k	Тур	e (66	1	19))													
	Connection Chunk Block Length																																				
	Initiator IP Address																																				
	Responder IP Address																																				
	Start Time																																				
														Aj	ppl	ica	tio	n]	ID																		
						R	esp	onc	ler	Po	rt								Pı	roto	ocol				(Coı	nne	ecti	on	Ту	ype						
											N	let]	Flo	W	De	tec	tor	II	P A	ddr	ess																
														F	Pacl	cet	s S	en	nt																		
													F	Pac	ket	s F	Rec	ei	ved																		
															Ву	tes	Se	nt	t																		
														Ву	tes	R	ece	iv	ed																		
														(Con	ne	ctio	on	.S																		

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

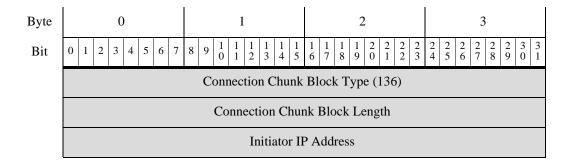
Table B-30 Connection Chunk Data Block Fields

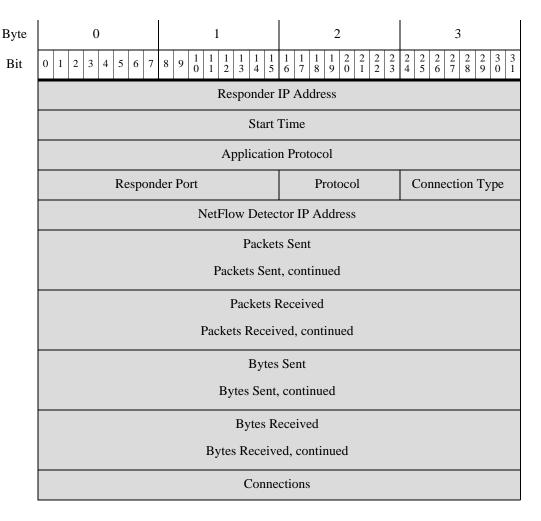
Field	Data Type	Description								
Connection Chunk Block Type	uint32	Initiates a Connection Chunk data block. This value is 66 for versions before 4.10.1 and a value of 119 for version 5.0.								
Connection Chunk Block Length	uint32	Total number of bytes in the Connection Chunk data block, including 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:





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

Table B-31 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.
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.

Table B-31 Connection Chunk Data Block Fields (continued)

Field	Data Type	Description
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-128.

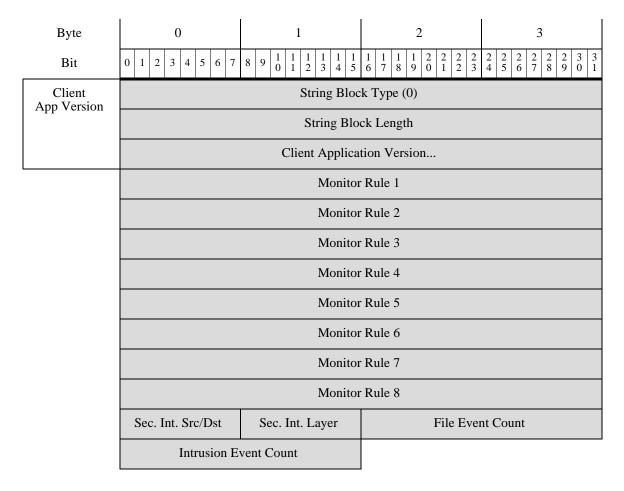
For more information on the Connection Statistics Data message, see Connection Statistics Data Message, page 4-51.

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

Byte			0		1										2	2								3	}						
Bit	0 1	2	3 4	5	6	7	8	9	10	1	1 1 1 2	1 3	- 4	1 1 4 5	1 6	7	1 1 7 8	1 9	(2 2	1	2 2	2 3	2 4	2 5	2 6	2 7	2 8	2 9	3	3
												Ing	gr	ess]	nte	erf	face														
										Ir	ngre	ss]	In	terfa	ice.	, (cont	inu	ie	d											
	Ingress Interface, continued																														
	Ingress Interface, continued																														
	Egress Interface continued																														
	Egress Interface, continued																														
	Egress Interface, continued																														
	Egress Interface, continued																														
	Initiator IP Address																														
	Initiator IP Address, continued																														
														Add																	
									Ir	ni				Ado						ed											
								,	,					nder																	
														P Ac																	
														P Ac																	
										-SI	POIN			icy F				<i>J</i> 110	.11.	ucu											
										P	Polic			evisi				nu	ec	1											
														evisi																	
														evisi																	
														Rul	e II)															
				I	Rul	e <i>A</i>	Acti	on													Rι	ıle	R	ea	son						
				I	niti	ato	or P	ort												R	es	po	nd	ler	Po	rt					
					TC	P]	Flag	gs									P	rot	to	col					Net	Fl	ow	So	our	ce	
										N	letF	lov	v S	Sou	ce,	, c	cont	inu	ied	d											
										N	letF	lov	v S	Sou	ce,	, c	cont	inu	ieo	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 NetFlow Sou	1 1 1 1 2 2 2 2 3 6 7 8 9 0 1 2 3 rce, continued	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1
	Ne	etFlow Source, continu		Instance ID
	Instance ID, cont.	Connection	on Counter	First Pkt Time
	First F	l Packet Timestamp, cor	ntinued	Last Pkt Time
	Last F	Packet Timestamp, cor	itinued	Initiator Tx Packets
		Initiator Transmitte	d Packets, continued	_
	Initiator	Transmitted Packets,	continued	Resp. Tx Packets
		Responder Transmit	ted Packets, continued	
	Responde	r Transmitted Packets	continued	Initiator Tx Bytes
		Initiator Transmitt	ed Bytes, continued	
	Initiator	Transmitted Bytes, c	ontinued	Resp. Tx Bytes
	Responder Transmitted Bytes, continued Responder Transmitted Bytes, continued			
				User ID
		User ID, continued		Application Prot. ID
Application Protocol ID, continued			ntinued	URL Category
	U	RL Category, continu	ed	URL Reputation
	UI	RL Reputation, contin	ued	Client App ID
	Clien	t Application ID, con	inued	Web App ID
Client URL	Web	Application ID, conti	nued	Str. Block Type (0)
OKL	Stri	String Block Type, continued		
	Strir	ng Block Length, conti	nued	Client App. URL
NetBIOS Name		String Blo	ck Type (0)	
Tuille		String Blo	ock Length	
		NetBIO	S Name	



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

Table B-32 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.
Egress Zone	uint8[16]	Egress security zone in the event that triggered the policy violation.
Ingress Interface	uint8[16]	Interface for the inbound traffic.
Egress Interface	uint8[16]	Interface for the outbound traffic.

Table B-32 Connection Statistics Data Block 5.1.1.x Fields (continued)

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

Table B-32 Connection Statistics Data Block 5.1.1.x Fields (continued)

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

Table B-32 Connection Statistics Data Block 5.1.1.x Fields (continued)

Field	Data Type	Description
Security Intelligence Source/ Destination	uint8	Whether the source or destination IP address matched the IP 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

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-134.

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

For more information on the Connection Statistics Data message, see Connection Statistics Data Message, page 4-51.

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

Byte	0	1	2	3
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1
		Connection Data l	Block Type (152)	
		Connection Data	a Block Length	
	Device ID			
	Ingress Zone			
	Ingress Zone, continued			
	Ingress Zone, continued			
	Ingress Zone, continued			
	Egress Zone			
		Egress Zone	e, 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 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	
	Egress Zone, continued				
		Egress Zone, continued			
		Ingress 1	Interface		
		Ingress Interfa	ace, continued		
		Ingress Interfa	ace, continued		
		Ingress Interfa	ace, continued		
		Egress I	nterface		
		Egress Interfa	ce, continued		
		Egress Interfa	ce, continued		
		Egress Interfa	ice, continued		
		Initiator IP Address			
	Initiator IP Address, continued				
		Initiator IP Add	lress, continued		
		Initiator IP Add	lress, continued		
		Responder	IP Address		
		Responder IP Ac			
	Responder IP Address, continued				
	Responder IP Address, continued				
	Policy Revision				
	Policy Revision, continued				
	Policy Revision, continued				
	Policy Revision, continued				
		Rule			
		Action	Rule R		
		or Port	Respond		
	TCP	Flags	Protocol	NetFlow Source	

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
	NetFlow Source, continued			
	NetFlow Source, continued			
		NetFlow Sou	rce, continued	
	Ne	etFlow Source, continu	ed	Instance ID
	Instance ID, cont.	Connection	on Counter	First Pkt Time
	First F	acket Timestamp, con	tinued	Last Pkt Time
	Last P	acket Timestamp, con	tinued	Initiator Tx Packets
		Initiator Transmitte	d Packets, continued	
	Initiator '	Transmitted Packets, c	ontinued	Resp. Tx Packets
	Responder Transmitted Packets, continued			
	Responder Transmitted Packets, continued			Initiator Tx Bytes
	Initiator Transmitted Bytes, continued			
	Initiator	Transmitted Bytes, co	ontinued	Resp. Tx Bytes
		Responder Transmit	ted Bytes, continued	
	Responder Transmitted Bytes, continued User ID			
	User ID, continued Application Pr ID			
	Applic	cation Protocol ID, con	tinued	URL Category
	U	RL Category, continue	ed	URL Reputation
	URL Reputation, continued Client A			Client App ID
	Clien	t Application ID, cont	inued	Web App ID
Client URL	Web	Application ID, conti	nued	Str. Block Type (0)
	Stri	ng Block Type, contin	ued	String Block Length
	Strin	g Block Length, conti	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 6 7 8 9 0 1 2 3	2 2 2 2 2 3 3 4 5 6 7 8 9 0 1
NetBIOS Name		String Bloc	ck Type (0)	
Ivaille		String Blo	ck Length	
		NetBIOS	Name	
Client App Version		String Bloc	ck 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 Eve	nt Count
	Intrusion E	vent Count	Initiator	Country
	Responde	r Country	IOC Number	
Source Autonomous System				
		Destination Auto	onomous System	
	SNM	IP In	SNM	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-33 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-33 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 o.	
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-33 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-33 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

Byte

Bit

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-149.

You request connection event records by setting the extended event flag—bit 30 in the Request Flags field—in the request message with an event version of 11 and an event code of 71. See Request Flags, page 2-11. If you enable bit 23, an extended event header is included in the record. For more information on the Connection Statistics Data message, see Connection Statistics Data Message, page 4-51.

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

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

Byte	0	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		
	Egress Interface					
	Egress Interface, continued					
	Egress Interface, continued					
	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			
		Policy R	evision			
		Policy Revision	on, continued			
		Policy Revision	on, continued			
		Policy Revision	on, continued			
		Rule	ID			
	Rule A	Action	Rule R	leason		
	Initiato	or Port	Respond	der Port		
	TCP	Flags	Protocol	NetFlow Source		
		NetFlow Sour	ce, continued			
	NetFlow Source, continued					
	NetFlow Source, continued					
	NetFlow Source, continued Instance ID					
	Instance ID, cont.	Connectio	n Counter	First Pkt Time		
	First P	acket Timestamp, cont	inued	Last Pkt Time		

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	
	Last 1	Initiator Tx Packets			
		Initiator Transmitted	Packets, continued		
	Initiator	Transmitted Packets, co	ontinued	Resp. Tx Packets	
		Responder Transmitte	ed Packets, continued		
	Responde	er Transmitted Packets,	continued	Initiator Tx Bytes	
		Initiator Transmitte	d Bytes, continued		
	Initiato	or Transmitted Bytes, con	ntinued	Resp. Tx Bytes	
		Responder Transmitt	ed Bytes, continued		
	Respond	ler Transmitted Bytes, co	ontinued	User ID	
		User ID, continued		Application Prot. ID	
	Appli	cation Protocol ID, cont	tinued	URL Category	
	Ţ	JRL Category, continue	d	URL Reputation	
	U	RL Reputation, continue	ed	Client App ID	
	Clie	Web App ID			
Client URL	We	b Application ID, contin	nued	Str. Block Type (0)	
	Str	ing Block Type, continu	ued	String Block Length	
	Stri	ng Block Length, contin	nued	Client App. URL	
NetBIOS Name		String Bloc	k Type (0)		
		String Bloo	ck Length		
	NetBIOS Name				
Client App Version String Block Type (0) String Block Length					
	Monitor Rule 2				

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 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 3				
	Monitor	Rule 4				
	Monitor	Rule 5				
	Monitor	Rule 6				
	Monitor	Rule 7				
	Monitor	Rule 8				
Sec. Int. Src/Dst	Sec. Int. Src/Dst Sec. Int. Layer File Event Count					
Intrusion E	vent Count	Initiator (Country			
Responde	r Country	IOC No	umber			
	Source Autono	omous System				
	Destination Auto	nomous System				
SNM	IP In	SNMP Out				
Source TOS	Destination TOS	Source Mask	Destination Mask			
	Security	Context				
	Security Context, continued					
Security Context, continued						
	Security Conte	ext, continued				

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

Table B-34 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-34 Connection Statistics Data Block 5.3.1 Fields (continued)

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

Table B-34 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-34 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-156.

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 2-11. If you enable bit 23, an extended event header is included in the record.

For more information on the Connection Statistics Data message, see Connection Statistics Data Message, page 4-51.

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

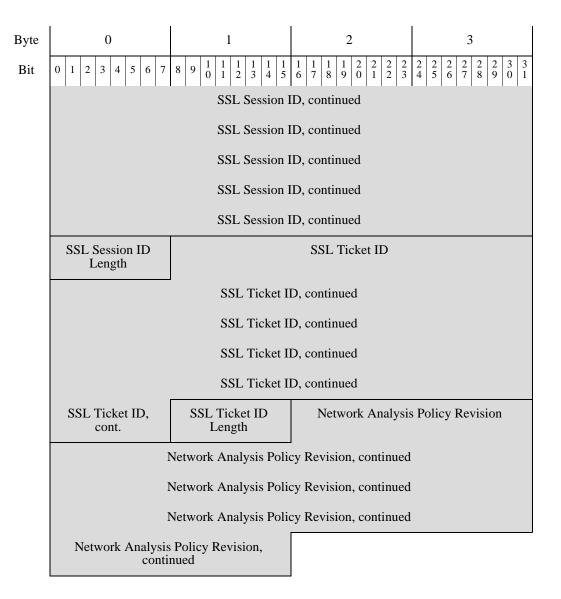
Byte	0	1	2	3			
Bit	0 1 2 3 4 5 6 7		1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1			
	Connection Data Block Type (155)						
	Connection Data Block Length						
	Device ID						
	Ingress Zone						
		Ingress Zone,	continued				
	Ingress Zone, continued						
	Ingress Zone, continued						
	Egress Zone						
	Egress Zone, continued						
	Egress Zone, continued						
	Egress Zone, continued						
		Ingress In	terface				
		Ingress Interfac	e, continued				
	Ingress Interface, continued						
	Ingress Interface, continued						
		Egress In	terface				
		Egress Interfac	e, 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			
	Egress Interface, continued						
	Egress Interface, continued						
		Initiator IF	Address				
		Initiator IP Add	ress, continued				
		Initiator IP Add	ress, continued				
		Initiator IP Add	ress, continued				
		Responder l	P Address				
		Responder IP Ad	dress, continued				
		Responder IP Add	dress, continued				
		Responder IP Ad	dress, continued				
	Policy Revision						
		Policy Revision	on, continued				
	Policy Revision, continued						
		Policy Revision	on, continued				
		Rule	ID				
	Rule A	Action	Rule R	Reason			
	Initiato	or Port	Respond	der Port			
	TCP I	Flags	Protocol	NetFlow Source			
		NetFlow Source	ce, continued				
		NetFlow Source	ce, continued				
	NetFlow Source, continued						
	NetFlow Source, continued Instance ID						
	Instance ID, cont. Connection Counter First Pk						
	First P	Packet Timestamp, cont	inued	Last Pkt Time			
	Last P	Packet Timestamp, cont	inued	Initiator Tx Packets			

Byte	0	1		2	3		
Bit	0 1 2 3 4 5 6 7 8	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1					
	Initiator Transmitted Packets, continued						
	Initiator Tı	ansmitted Packet	s, continue	d	Resp. Tx Packets		
	Responder Transmitted Packets, continued						
	Responder 7	Transmitted Pack	ets, continu	ied	Initiator Tx Bytes		
		Initiator Transn	nitted Bytes	s, continued			
	Initiator T	ransmitted Bytes	, continued	l	Resp. Tx Bytes		
		Responder Trans	mitted Byt	es, continued			
	Responder	Transmitted Byte	es, continue	ed	User ID		
		User ID, continue	ed		Application Prot. ID		
	Applicat	ion Protocol ID,	continued		URL Category		
	UR	L Category, conti	nued		URL Reputation		
	URL	Client App ID					
	Client A	Web App ID					
	Web A	application ID, co	ntinued		Str. Block Type (0)		
Client URL	String	g Block Type, con	ntinued		String Block Length		
	String	Block Length, co	ntinued		Client App. URL		
S		String I	Block Type	(0)			
NetBIOS Name		String	Block Leng	gth			
Z	NetBIOS Name						
t sion		String I	Block Type	(0)			
Client App Version		String	Block Leng	gth			
Ap]		Client App	lication Ve	ersion			
		Mor	itor Rule 1				
		Mor	itor Rule 2				
		Mor	itor Rule 3				

	Byte	0	1	2 3							
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 String Block Type (0) String Block Length User Agent	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						
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, continued String Block Type (0) String Block Length String Block Length User Agent		Monitor Rule 4									
Monitor Rule 7 Monitor Rule 8 Sec. Int. Src/Dst Sec. Int. Layer File Event Count Intrusion Event Count Responder 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 String Block Type (0) String Block Length String Block Length User Agent		Monitor Rule 5									
Sec. Int. Src/Dst Sec. Int. Layer File Event Count Intrusion Event Count Intrusion Event Count Responder 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 String Block Type (0) String Block Length String Block Length String Block Length User Agent			Monitor	Rule 6							
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 Security Context, continued Security Context, continued Security Context, continued String Block Type (0), continued String Block Length String Block Length, continued String Block Length User Agent			Monitor	Rule 7							
Intrusion Event Count Responder Country Responder Country IOC Number Source Autonomous System Destination Autonomous System SNMP In Source TOS Destination TOS Source Mask Destination Mask Security Context Security Context, continued Security Context, continued Security Context, continued Security Context, continued Security Context, continued String Block Type (0) String Block Length String Block Length User Agent			Monitor	· Rule 8							
Responder Country FOR Number Source Autonomous System Destination Autonomous System SNMP In SOURCE TOS Destination TOS Source Mask Security Context Security Context, continued String Block Type (0) String Block Type (0), continued String Block Length String Block Length String Block Type (0) String Block Type (0) String Block Length User Agent		Sec. Int. Src/Dst	Sec. Int. Layer	File Eve	nt Count						
Source Autonomous System Destination Autonomous System		Intrusion E	vent Count	Initiator	Country						
SNMP In SNMP Out		Responde			umber						
SNMP In SNMP Out Source TOS Destination TOS Source Mask Destination Mask Security Context Security Context, continued String Block Type (0) String Block Type (0), continued String Block Length String Block Length, continued Referenced Host String Block Length User Agent											
Source TOS Destination TOS Source Mask Destination Mask Security Context Security Context, continued String Block Type (0) String Block Type (0), continued String Block Length String Block Length, continued String Block Type (0) String Block Length User Agent											
Security Context Security Context, continued Security Context, continued Security Context, continued Security Context, continued Security Context, continued String Block Type (0) String Block Type (0), continued String Block Length String Block Length, continued Referenced Host String Block Type (0) String Block Length User Agent											
Security Context, continued String Block Type (0) String Block Type (0) String Block Length String Block Length, continued Referenced Host String Block Type (0) String Block Length User Agent		Source TOS			Destination Mask						
Security Context, continued Security Context, continued VLAN ID String Block Type (0) String Block Type (0), continued String Block Length String Block Length, continued Referenced Host String Block Type (0) String Block Length User Agent											
Security Context, continued VLAN ID String Block Type (0) String Block Type (0), continued String Block Length String Block Length, continued Referenced Host String Block Type (0) String Block Length User Agent											
VLAN ID String Block Type (0) String Block Type (0), continued String Block Length String Block Length, continued Referenced Host String Block Type (0) String Block Type (0) User Agent											
String Block Type (0), continued String Block Length String Block Length, continued Referenced Host String Block Type (0) String Block Type (0) User Agent	tt.	VLA			ek Type (0)						
String Block Length, continued Referenced Host String Block Type (0) String Block Length User Agent	зоН ра										
String Block Type (0) String Block Length User Agent	erence										
String Block Length User Agent	Ref										
	gent		String Block Type (0)								
	ser Ag	String Block Length									
String Block Type (0) String Block Length	ñ	User Agent									
String Block Length	errer		String Block Type (0)								
	'P Ref										
HTTP Referrer	НТТ		HTTP R	eferrer							

Byte	0							1						2							3											
Bit	0 1	0 1 2 3 4 5 6 7 8 9 1 1 2 3 4 5 6 7 8 9 1 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																														
	SSL Certificate Fingerprint																															
	SSL Certificate Fingerprint, continued																															
									S	SSL	Ce	rt	ifica	ite]	Fir	nge	rpri	in	it, co	onti	'n	uec	l									
									S	SSL	Ce	rt	ifica	ite l	Fii	ige	rpri	in	it, co	onti	'n	uec	[
									S	SSL	Ce	rt	ifica	ite]	Fir	nge	rpri	in	it, co	onti	in	uec	<u> </u>									
													S	SL	Po	olic	y I	D)													
											S	S	L Po	olic	y]	D,	COI	nt	inue	ed												
											S	S	L Po	olic	y]	D,	COI	nt	inue	ed												
											S	S	L Po						inue	ed												
														SSL	. F	Rule								1								
							Cipł	ner		Suite	<u> </u>								SL V	ers	sic	on		SSL Srv Cert. Stat.								
	S		Srv at., o										SSI	. A	ctı	ıal	Ac	ti	on							SS			ior	cte	d	
	SSL Expected SSL Flow Status SSL Flow Error Action, cont.																															
	SSL Flow Error, continued SSL Flow Messages SSL Flow Messages, continued SSL Flow Flags SSL Flow Flags, continued SSL Flow Flags, continued String Block Type (0) String Block Type (0), continued String Block Length																															
ames									ock))	ς Τ <u>΄</u>	ype																					
SSL Server Names																																
SSF S	String Block Length, continued SSL Server Name																															
	SSL URL Category																															
	SSL Session ID																															
											SS	SI	L Se	ssic	n	ID,	co	n	tinu	ed												
											SS	SI	L Se	ssic	n	ID,	co	n	tinu	ed												



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

Table B-35 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-35 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-35 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-35 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-35 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-35 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-35 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-35 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-35	Connection Statistics Data Block 5.4+ Fields (continued)
า สมเย อ-งจ	Connection Statistics Data Block 3.4+ 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.

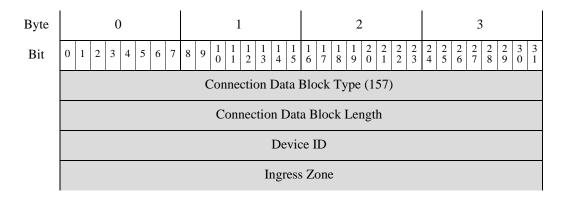
Connection Statistics Data Block 5.4.1

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-156.

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 2-11. If you enable bit 23, an extended event header is included in the record.

For more information on the Connection Statistics Data message, see Connection Statistics Data Message, page 4-51.

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



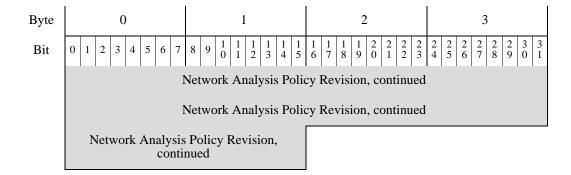
Byte	0			1					2					3										
Bit	0 1 2	3 4	5	6 7	8	9 1	1	1 2	1 3	1 4	1 5	1 1 6 7	1 8	2 0	2	2 2	2 3	2 4	2 2 6	2 7	2 8	2 9	3	3
			,			,	I	ng	ress	Z	one	, con	tinue	ed						,		,	,	
	Ingress Zone, continued																							
	Ingress Zone, continued																							
	Egress Zone																							
	Egress Zone, continued																							
	Egress Zone, continued Egress Zone, continued																							
	Ingress Interface																							
	Ingress Interface, continued																							
	Ingress Interface, continued																							
	Ingress Interface, continued																							
	Egress Interface Egress Interface, continued Egress Interface, continued Egress Interface, continued																							
	Initiator IP Address																							
												ess,												
												ess,												
]						ess,			d									
						ъ			_			P Ad												
	Responder IP Address, continued Responder IP Address, continued Responder IP Address, continued																							
	Policy Revision																							
	Policy Revision, continued																							
	Policy Revision, 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						
	Policy Revision, continued									
	Rule ID									
	Rule A	Leason								
	Initiato	ler Port								
	TCP I	NetFlow Source								
	NetFlow Source, continued									
	Ne	Instance ID								
	Instance ID, cont.	Instance ID, cont. Connection Counter								
	First P	Last Pkt Time								
	Last P	Initiator Tx Packets								
	Initiator '	Resp. Tx Packets								
	Responder	Initiator Tx Bytes								
	Initiator	Resp. Tx Bytes								
	Responder Transmitted Bytes, continued									
	Responde	User ID								
		Application Prot. ID								
	Applic	URL Category								
	U	URL Reputation								
	UF	Client App ID								
	Clien	Web App ID								

Byte	0	1	2	3								
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 1 2 2 2 2 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	Str. Block Type (0)										
Client URL	Stri	String Block Length										
	Strin	g Block Length, contir	nued	Client App. URL								
S	String Block Type (0)											
NetBIOS Name	String Block Length											
Ž	NetBIOS Name											
ion		String Bloc	String Block Type (0)									
Client App Version		k Length										
App		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	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 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 Context, continued										
	Security Context, continued										
	Security Context, continued										
Referenced Host	VLA	N ID	String Block Type (0)								
	String Block Typ	pe (0), continued	String Block Length								
	String Block Le	ngth, continued	Referenced Host								
ent	String Block Type (0)										
User Agent	String Block Length										
Use	User Agent										
rrer	String Block Type (0)										
Refe	String Block Length										
HTTP Referrer	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	ner Suite	SSL Version SSL Srv Cert. Sta								
	SSL Srv Cert. Stat., cont.	al Action	SSL Expected Action								

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							
	SSL Expected Action, cont.	SSL Flow Error									
	SS	SSL Flow Messages									
	SSL	SSL Flow Flags									
		SSL Flow Fla	gs, continued								
ames	SS	String Block Type (0)									
SSL Server Names	String	inued	String Block Length								
STSS	Strin	nued	SSL Server Name								
	SSL URL Category										
	SSL Session ID										
		SSL Session 1	ID, continued								
		SSL Session l	ID, continued								
		SSL Session 1	ID, continued								
		SSL Session 1	ID, continued								
		SSL Session 1	ID, continued								
		SSL Session 1	ID, continued								
		SSL Session 1	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 Network Analysis Policy Revision										
]	Network Analysis Poli	cy Revision, continued								



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

Table B-36 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.
TCP Flags	uint16	Indicates any TCP flags for the connection event.
Protocol	uint8	The IANA-specified protocol number.

Table B-36 Connection Statistics Data Block 5.4+ Fields (continued)

Field	Data Type	Description							
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 o.							
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-36 Connection Statistics Data Block 5.4+ Fields (continued)

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

Table B-36 Connection Statistics Data Block 5.4+ Fields (continued)

Field	Data Type	Description
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.
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.

Table B-36 Connection Statistics Data Block 5.4+ Fields (continued)

Field	Data Type	Description
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.
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-36 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-36 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.

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	uint8	Length of the SSL Ticket ID. While the ticket ID cannot exceed 20

bytes, it may be less than 20 bytes.

Revision of the Network Analysis Policy associated with the

Table B-36 Connection Statistics Data Block 5.4+ Fields (continued)

Connection Statistics Data Block 6.0.x

Policy revision

Network Analysis

uint8[16]

Length

7

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-176. 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 2-11. 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:

connection event.

Byte	0							1					2					3										
Bit	0 1 2 3 4 5 6 7					7	8	9	1	1	1 2	1 3	1 4	1 5	1 6	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3				2 3	2 4	2 5	2 6	2 7	2 8	2	3	3
		Connection Statistics Data Block Type (160)																										
	Connection Statistics Data Block Length																											
	Device ID																											
	Ingress Zone																											
	Ingress Zone, continued																											

Byte	0	1			2		3						
Bit	0 1 2 3 4 5 6 7	8 9 1 1 2	$\begin{array}{c cccc} 1 & 1 & 1 \\ 2 & 3 & 4 \end{array}$	1 1 1 5 6 7	1 1 2 8 9 0	2 2 1 2	2	2 2 4 5	6	2 2 2	2 2 9	3 3	3
		Ing	gress Zo	ne, con	tinued						,		
		Ing	gress Zo	one, con	tinued								
	Egress Zone												
	Egress Zone, continued												
	Egress Zone, continued												
	Egress Zone, continued												
	Ingress Interface												
	Ingress Interface, continued												
	Ingress Interface, continued												
	Ingress Interface, continued												
	Egress Interface												
		Egre	ess Inter	face, co	ontinued								
		Egre	ess Inter	face, co	ontinued								
		Egre	ess Inter	face, co	ntinued								
			Initiator	IP Add	ress								
			tor IP A										
		Initiat	tor IP A	ddress,	continue	ed							
			tor IP A			ed							
			Responde										
			nder IP A										
			nder IP A										
		Respon	nder IP A			ıed							
			·	Revisi									
			icy Revi										
			icy Revi										
		Poli	icy Revi	sion, co	ntinued								

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	ID									
	Rule A	Action	Rule Reason									
	Rule Reas	son, cont.	Initiato	or Port								
	Respond	der Port	TCP I	Flags								
	Protocol		NetFlow Source									
	NetFlow Source, continued NetFlow Source, continued											
		NetFlow Sour	ce, continued									
	NetFlow Src, cont.	e, cont. Instance ID Connection Counter										
	Cx Counter, cont.	First Packet Timestamp										
	First Pkt Time, cont.	Last Packet Timestamp										
	Last Pkt Time, cont.	Init	iator Transmitted Pack	ets								
		Initiator Transmitted	Packets, continued									
	Initiator Tx Pkt, cont.	Resp	onder Transmitted Pac	kets								
		Responder Transmitte	ed Packets, continued									
	Res. Tx Pkts, cont.	Ini	tiator Transmitted Byte	es								
		Initiator Transmitte	d Bytes, continued									
	Initiator Tx Bts, cont.	Res	ponder Transmitted By	rtes								
		Responder Transmitt	ed Bytes, continued									
	Res. Tx Bts, cont.		User ID									
	User ID, continued	A	application Protocol ID									
	App Prot ID, cont.		URL Category									
	URL Category, cont.		URL Reputation									

Byte		0									1				2 3																	
Bit	0 1	2	3	4	5	6	7	8	9	1	1 1		1 2	1 1 3 4			1 1 6 7	1 8	3 9	2 0	2	2 2	$\begin{bmatrix} 2 & 2 \\ 2 & 3 \end{bmatrix}$		2	2 5	2 6	2 7	2 8	2 9	3	3 1
	UI	RL	Re	ep,	co	nt.										(Clier	nt A	Ap	plic	ati	ion	ID									
	C	lier		Ap nt.		D,											Web	A	App	olica	tic	on	ID									
	Wel	b A	pp	II (Э, с	ont										S	tring	g. I	Blo	ock	Ту	/pe	(0))								
Client URL	Str	Str. Block Type, cont.														Striı	ng .	Bl	ock	L	eng	gth										
	St	Str. Block Len., cont.														Clie	ent	t A	pp.	Ul	RL											
S								String Block Type (0)																								
NetBIOS Name								String Block Length																								
Z													N	etB	Ю	S	Nan	ıe	••													
t sion												S	tri	ng E	3 1c	ock	Ту	pe	(0)												
Client App Version													Str	ing	B1	loc	k Le	eng	gth													
Ap											Cli	ier					ion '		rsi	on	•											
																	Rule															
																	Rule															
																	Rule															
																	Rule															
														Mon	ito	or	Rule	5														
																	Rule															
																	Rule															
	Sa	Monitor Rule 8 Sec. Int. Src/Dst Sec. Int. Layer File Event Count																														
	36	. I	.111.				, E	7701			ount		La	.yeı		-																
					Res																		ator C N									
					·cs	POI	ıuc	, C	υι	110		ıır	rce	Am	tot	no	mou	s S	Sve	tem		10	C I	1 U	111	<i>J</i> C1						
										Γ							nom					1										
	SNM				1P	[n	L	. 031.	.110	at1'		<u>.u</u>	101	.OIII	Jui	o N	Jan	J111		NM	P	0	11f									
		SN				111																. 1111		J	٠,٠							

Byte	0	1				2					3		
Bit	0 1 2 3 4 5 6 7		1 1 4 5	1 1 6 7	1 8	1 2 9 0	2	2 2 3	2 4	2 2 5 6	2 7	2 2 9	3 3 0 1
	Source TOS	Destination TO	S	S	Soui	rce M	lask		Г	Destir	natio	n M	ask
		Security Context											
		Security (Cont	ext, co	onti	nued							
		Security (Cont	ext, co	onti	nued							
		Security (Cont	ext, co	onti	nued							
Host	VLA	N ID				Stı	ring	Bloc	k T	ype	(0)		
nced F	String Block Typ	String Block Length											
Referenced Host	String Block Le	Referenced Host											
ent		String	Bloc	ek Typ	pe (0)							
User Agent		String	Blo	ck Le	ngt	h							
Use		Us	er A	gent.	••								
ırer		String	Bloo	k Typ	pe (0)							
HTTP Referrer		String	Blo	ck Le	ngt	h							
HTT		НТТ	ΥR	eferre	er								
		SSL Cert	ifica	te Fin	ger	print							
		SSL Certificate	Fin	gerpr	int,	conti	inue	d					
		SSL Certificate	Fin	gerpr	int,	conti	inue	d					
		SSL Certificate	Fin	gerpr	int,	conti	inue	d					
		SSL Certificate	Fin	gerpr	int,	conti	inue	d					
		SSL Policy ID											
	SSL Policy ID, continued												
		SSL Pol											
		SSL Pol				ued							
		SSL Rule ID											
	SSL Cipl	er Suite	SSL Cipher Suite SSL Version SSL Srv Cert. Stat.										

Byte		0										1					2					3									
Bit	0	1 2	3	4	1 5	6	7	8	9	1	1 1	1 2	1 3		1 5	1 6	1 7	1 8	1 9	2 0	2	2 2	2 3	2 4	2 5	2 6		2 2 2 7 8	2 2 9	3	3
		SSL Srv Cert. Stat., cont.							SSL Actual Action								S			Exp	ecte	ed									
		SSL Act	Eior	xp	ecte	ed i.						i	SS	SL I	Flo	w S	tat	tus							SS	L	F	low	En	or	
							SSI	L I	Flo	w	En	ror,	, c	onti	nu	ed												L Fl	low ges		
						SS	SL F	Flo	ow	M	ess	sage	es,	, co	ntiı	nue	d								SS	L I	Fl	low	Fla	ıgs	
											SS	SL I	Fl	ow i	Fla	gs,	со	nti	nue	ed											
ames							SSI	Ŀ	Flo	w	Fla	ıgs,	, c	onti	nu	ed								S	Stri	ng		3loc (0)	k T	ype	e
SSL Server Names						Str	ing	B	loc	k '	Туј	pe ((0)), cc	onti	nu	ed								S			g B eng	locl th	X.	
SSF S						St	ring	g E	Blo	ck	Le	engt	th,	, co	ntiı	nue	d							SSL Server Name							
												S	SI	L U	RL	Ca	teg	gor	y												
													S	SL	Ses	sio	n I	D													
											SS	SL :	Se	essio	on l	D,	со	nti	nue	d											
											SS	SL	Se	essio	on]	D,	co	nti	nue	ed											
											SS	SL :	Se	essio	on]	D,	co	nti	nue	ed											
											SS	SL	Se	essio	on]	D,	co	nti	nue	d											
											SS	SL	Se	essio	on]	D,	co	nti	nue	ed											
											SS	SL	Se	essio	on]	D,	co	nti	nue	ed											
											SS	SL :	Se	essio	on]	D,	co	nti	nue	d											
		SSL 1	Se Lei			ID											SS	SL	Tic	ke	t II)									
											S	SL	T	icke	et I	D,	coı	ntin	ue	d											
											S	SL	T	icke	et I	D,	coı	ntin	ue	d											
											S	SL	T	icke	et I	D,	coi	ntin	ue	d											
											S	SL	T	icke	et I	D,	coı	ntin	ue	d											

Byte	0	1			2			3							
Bit	0 1 2 3 4 5 6 7	8 9 1 1	$\begin{array}{c ccc} 1 & 1 & 1 \\ 2 & 3 & 4 \end{array}$	1 5	1 1 6 7		1 2 0	2 2 1 2	2	2 2	2 2 6	2 7	2 8 9	3 0	3
	SSL Ticket ID, cont.	SSL Tic			1	Netv	vork	Analy	sis	Pol	licy	Rev	isior	1	
	1	Vetwork An	alysis Po	olic	y Re	visio	on, c	ontinue	ed						
	ı	olic	licy Revision, continued												
	1	Jetwork An	alysis Po	olic	icy Revision, continued										
	Network Analysis contin		ision,		Endpoint Profile ID										
	Endpoint Profile		Security Group ID												
	Security Group					Locat	io	n IP	v6						
		Lo	ocation I	Pve	v6, continued										
			ocation I												
		Lo	ocation I	Pv6	5, cor	ntinu	ied								
	Location IPv	5, continued	1		HTTP Response										
	HTTP Respon	se, continue	ed		String Block Type (0)										
	String Block Typ	e (0), conti	nued		String Block Length										
	String Block Le	ngth, contin	ued					DNS	Q	uery	/ 				
	DNS Rec	ord Type					D	NS Res	spo	onse	Ty	pe			
			DN	IS '	ΓTL										
			Sinkh	ole UUID											
		UID, continued													
		nkhole U	UID, continued												
		nkhole U	UI	D, co	ntin	ued									
		Sec	curity Int	ell	igenc	e Li	st 1								
		curity Int	ell	igenc	e Li	st 2									

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

Table B-37 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-37 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-37 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-37 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-37 Connection Statistics Data Block 6.0.x Fields (continued)

Field	Data Type	Description
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.
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-37 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:
		• 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-37 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 0.

Table B-37 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-37 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	
		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.	

Legacy File Event Data Structures

The following topics describe other legacy file event data structures:

- File Event for 5.1.1.x, page B-205
- File Event for 5.2.x, page B-209
- File Event for 5.3, page B-213

- File Event for 5.3.1, page B-219
- File Event for 5.4.x, page B-225
- File Event SHA Hash for 5.1.1-5.2.x, page B-235

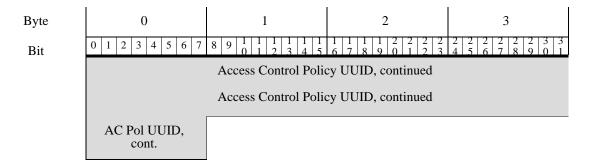
File Event for 5.1.1.x

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 2 2 2 2 2 2 2				
	File Event Block Type (23)				
	File Event Block Length				
		Devic	ee 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 Ad	ldress, continued		
	Destination IP Address, continued				
	Destination IP Address, continued				
	Disposition	Action	SHA	Hash	

Byte Bit	0 0 1 2 3 4 5 6 7	1 8 9 1 1 1 1 1 1 1 1 1 5	continued continued continued continued continued continued	3 2 2 2 2 3 3 3 6 7 8 9 0 1	
	SHA Hash,	, continued	File Type ID		
File Name	File Type	ID, cont.	String Block Type	e (0)	
	String Block Type (0), cont. String Block Length			gth	
	String Block Length, cont. File Name				
		File	Size		
		File Size,	continued		
	Direction		Application ID		
	App ID, cont.		User ID		
URI	User ID, cont.		String Block Type (0)		
	String Block Type (0), cont.		String Block Length		
	String Block Length, cont.	URI			
Signature		String Block Type (0)			
		String Blo	ck Length		
	Signature				
	Source	e Port	Destination Po	rt	
	Protocol	Acc	ess Control Policy UUID		
	Access Control Policy UUID, continued				



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

Table B-38 File Event Data Block Fields

Field	Data Type	Description		
File Event Block Type	uint32	Initiates whether file event data block. This value is always 23.		
File Event Block Length	uint32	Total number of bytes in the file event block, including eight bytes for the file event block type and length fields, plus the number of bytes of data that follows.		
Device ID	uint32	ID for the device that generated the event.		
Connection Instance	uint16	Snort instance on the device that generated the event. Used to link the event with a connection or intrusion event.		
Connection Counter	uint16	Value used to distinguish between connection events that happen during the same second.		
Connection Timestamp	uint32	UNIX timestamp (seconds since 01/01/1970) of the associated connection event.		
File Event Timestamp	uint32	UNIX timestamp (seconds since 01/01/1970) of when the file type is identified and the file event generated.		
Source IP Address	uint8[16]	IPv4 or IPv6 address for the source of the connection.		
Destination IP Address	uint8[16]	IPv4 or IPv6 address for the destination of the connection.		
Disposition	uint8	The malware status of the file. Possible values include:		
		• 1 — CLEAN — The file is clean and does not contain malware.		
		• 2 — UNKNOWN — It is unknown whether the file contains malware.		
		• 3 — MALWARE — The file contains malware.		
		• 4 — CACHE_MISS — The software was unable to send a request to the Cisco cloud for a disposition.		
		• 5 — NO_CLOUD_RESP — The Cisco cloud services did not respond to the request.		

Table B-38 File Event Data Block Fields (continued)

Field	Data Type	Description
Action	uint8	The action taken on the file based on the file type. Can have the following values:
		• 1 — Detect
		• 2 — Block
		• 3 — Malware Cloud Lookup
		• 4 — Malware Block
		• 5 — Malware 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.
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.

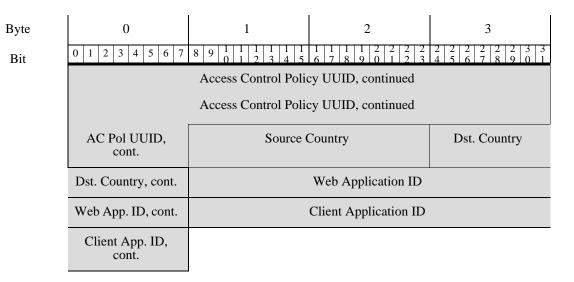
File Event for 5.2.x

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 1 1 1 1 1 1 2 2 2 2 2 2				
	File Event Block Type (32)				
	File Event Block Length				
		Devic	ee ID		
	Connection	n Instance	Connection	n Counter	
		Connection	Timestamp		
	File Event Timestamp				
	Source IP Address				
	Source IP Address, continued				
	Source IP Address, continued				
		Source IP Addr	ess, continued		
		Destination	IP Address		
		Destination IP Ad	ldress, continued		
	Destination IP Address, continued				
	Destination IP Address, continued				
	Disposition	Action	SHA	Hash	

Byte	0	1	2	3	
Bit	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				
	SHA Hash, continued				
	SHA Hash, continued				
		SHA Hash,			
		SHA Hash,			
		SHA Hash,			
		SHA Hash,			
		SHA Hash,	, continued		
	SHA Hash	, continued	File T	ype ID	
File Name	File Type	ID, cont.	String Bloo	ck Type (0)	
	String Block	Гуре (0), cont.	String Blo	String Block Length	
	String Block Length, cont. File Name		Jame		
	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				
	Sourc	e Port	Destinat	tion Port	
	Protocol	Acc	cess Control Policy UU	JID	
	Access Control Policy UUID, continued				



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

Table B-39 File Event Data Block Fields

Field	Data Type	Description		
File Event Block Type	uint32	Initiates whether file event data block. This value is always 23.		
File Event Block Length	uint32	Total number of bytes in the file event block, including eight bytes for the file event block type and length fields, plus the number of bytes of data that follows.		
Device ID	uint32	ID for the device that generated the event.		
Connection Instance	uint16	Snort instance on the device that generated the event. Used to link the event with a connection or intrusion event.		
Connection Counter	uint16	Value used to distinguish between connection events that happen during the same second.		
Connection Timestamp	uint32	UNIX timestamp (seconds since 01/01/1970) of the associated connection event.		
File Event Timestamp	uint32	UNIX timestamp (seconds since 01/01/1970) of when the file type is identified and the file event generated.		
Source IP Address	uint8[16]	IPv4 or IPv6 address for the source of the connection.		
Destination IP Address	uint8[16]	IPv4 or IPv6 address for the destination of the connection.		

Table B-39 File Event Data Block Fields (continued)

Field	Data Type	Description
Disposition	uint8	The malware status of the file. Possible values include:
		• 1 — CLEAN — The file is clean and does not contain malware.
		• 2 — NEUTRAL — It is unknown whether the file contains malware.
		• 3 — MALWARE — The file contains malware.
		• 4 — CACHE_MISS — The software was unable to send a request to the Cisco cloud for a disposition, or the Cisco cloud services did not respond to the request.
Action	uint8	The action taken on the file based on the file type. Can have the following values:
		• 1 — Detect
		• 2 — Block
		• 3 — Malware Cloud Lookup
		• 4 — Malware Block
		• 5 — Malware 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-39 File Event Data Block Fields (continued)

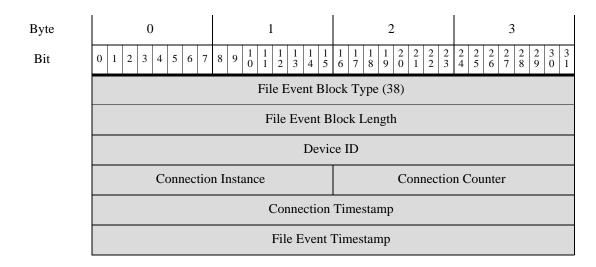
Field	Data Type	Description
Protocol	uint8	IANA protocol number specified by the user. For example:
		• 1 — ICMP
		• 4 — IP
		• 6 — TCP
		• 17 — UDP
		This is currently only TCP.
Access Control Policy UUID	uint8[16]	Unique identifier for the access control policy that triggered the event.
Source Country	uint16	Code for the country of the source host.
Destination Country	uint16	Code for the country of the destination host.
Web Application ID	uint32	The internal identification number for the web application, if applicable.
Client Application ID	uint32	The internal identification number for the client application, if applicable.

File Event for 5.3

The file event contains information on files that are sent over the network. This includes the connection information, whether the file is malware, and specific information to identify the file. The file event has a block type of 38 in the series 2 group of blocks. It supersedes block type 32. New fields have been added to track dynamic file analysis and file storage.

You request file event records by setting the file event flag—bit 30 in the Request Flags field—in the request message with an event version of 3 and an event code of 111. See Request Flags, page 2-11. If you enable bit 23, an extended event header is included in the record.

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



Byte	0	1	2	3		
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1		
	Source IP Address					
	Source IP Address, continued					
		Source IP Address, continued				
	Source IP Address, continued					
		Destination IP Address				
		Destination IP Ac	ddress, continued			
		Destination IP Ac	ddress, continued			
		Destination IP Ac	ldress, 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), 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	ek Type (0)	
		String Blo	ck Length	
	Signature			
	Source Port Destination Port			ion Port
	Protocol	Access Control Policy UUID		
		Access Control Policy 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.			

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

Table B-40 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-40 File Event Data Block Fields (continued)

Field	Data Type	Description
Connection Counter	uint16	Value used to distinguish between connection events that happen during the same second.
Connection Timestamp	uint32	UNIX timestamp (seconds since 01/01/1970) of the associated connection event.
File Event Timestamp	uint32	UNIX timestamp (seconds since 01/01/1970) of when the file type is identified and the file event generated.
Source IP Address	uint8[16]	IPv4 or IPv6 address for the source of the connection.
Destination IP Address	uint8[16]	IPv4 or IPv6 address for the destination of the connection.
Disposition	uint8	The malware status of the file. Possible values include:
		• 1 — CLEAN The file is clean and does not contain malware.
		• 2 — UNKNOWN It is unknown whether the file contains malware.
		• 3 — MALWARE The file contains malware.
		 4 — UNAVAILABLE The software was unable to send a request to the Cisco cloud for a disposition, or the Cisco cloud services did not respond to the request.
		• 5 — CUSTOM SIGNATURE The file matches a user-defined hash, and is treated in a fashion designated by the user.
SPERO Disposition	uint8	Indicates whether the SPERO signature was used in file analysis. If the value is 1, 2, or 3, SPERO analysis was used. If there is any other value SPERO analysis was not used.
File Storage Status	uint8	The storage status of the file. Possible values are:
		• 1 — File Stored
		• 2 — File Stored
		• 3 — Unable to Store File
		• 4 — Unable to Store File
		• 5 — Unable to Store File
		• 6 — Unable to Store File
		• 7 — Unable to Store File
		• 8 — File Size is Too Large
		• 9 — File Size is Too Small
		• 10 — Unable to Store File
		• 11 — File Not Stored, Disposition Unavailable

Table B-40 File Event Data Block Fields (continued)

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		
	 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 		
	 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 		
	 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 		
	 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 		
	 6 — Failed to Send 7 — Failed to Send 8 — Failed to Send 9 — File Size is Too Small 10 — File Size is Too Large 		
	 7 — Failed to Send 8 — Failed to Send 9 — File Size is Too Small 10 — File Size is Too Large 		
	 8 — Failed to Send 9 — File Size is Too Small 10 — File Size is Too Large 		
	 9 — File Size is Too Small 10 — File Size is Too Large 		
	• 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 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.		

Table B-40 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 3-39 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

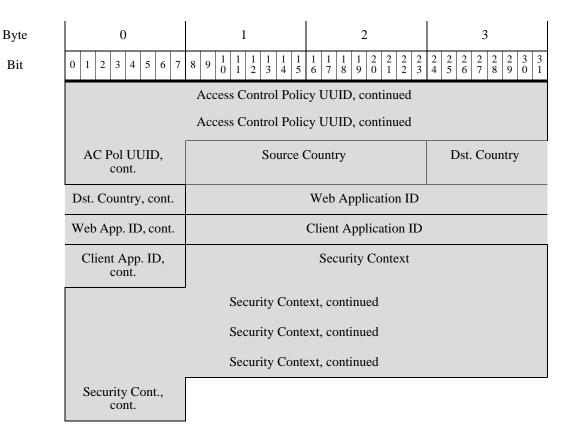
The file event contains information on files that are sent over the network. This includes the connection information, whether the file is malware, and specific information to identify the file. The file event has a block type of 43 in the series 2 group of blocks. It supersedes block type 38. A security 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 2-11. If you enable bit 23, an extended event header is included in the record.

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

Byte	0	1	2	3	
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1	
		File Event Blo	ock Type (43)		
		File Event B	lock Length		
		Devi	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 1 1 1 1 1 1 2 2 2 2 2 3 2		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, continued				
		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), cont. String Block Length				
	String Block Length, cont. File Name				
	File Size				
	File Size, continued				
	Direction Application ID				
	App ID, cont.	User ID			
URI	User ID, cont.		String Block Type (0)		
	String Block Type (0), cont.		String Block Length		
	String Block Length, cont.	URI			
Signature	String Block Type (0)				
	String Block Length				
	Signature				
	Sourc	e Port	Destinat	tion Port	
	Protocol	Acc	cess Control Policy UU	JID	
	Access Control Policy UUID, continued				



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

Table B-41 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-41 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-41 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 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
		Transmit Not Send Sendbox Private Cloud - File not send to the private cloud for analysis Firepower eStreamer integration Guide

Table B-41 File Event Data Block Fields (continued)

Field	Data Type	Description		
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.		
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 3-39 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-41 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 2-11. If you enable bit 23, an extended event header is included in the record.

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

Byte	0 1 2 3				
Bit	0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2				
	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 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		
	Source IP Address					
	Source IP Address, continued					
	Source IP Address, continued					
	Source IP Address, continued					
	Destination IP Address					
		Destination IP Ac	ddress, continued			
		Destination IP Ac	ddress, continued			
		Destination IP Ac	ddress, continued			
	Disposition SPERO File Storage Status File Analysis Status					
	Archive File Status	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				String Block Type (0)		
	String Block Type (0), cont. String Block Length					
	St	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 1 1 1 1 1 2 2 2 2 2 2 2		
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 Bloo	ck Length	
		Signat	ure	
	Source	e Port	Destinat	ion Port
	Protocol	Acc	ess Control Policy UU	JID .
		Access Control Policy UUID, continued		
		Access Control Policy UUID, continued		
		Access Control Policy UUID, continued		
	AC Pol UUID, cont.	Source Country Dst. Country		Dst. Country
	Dst. Country, cont.	Web Application ID		
	Web App. ID, cont.		Client Application ID	
	Client App. ID, cont.		Security Context	
		Security Conte	ext, continued	
		Security Conte	ext, continued	
		Security Conte	ext, continued	
	Security Cont., SSL Certificate Fingerprint cont.			nt
		SSL Certificate Fingerprint, continued		
		SSL Certificate Fingerprint, continued		
		SSL Certificate Fingerprint, 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 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	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				

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

Table B-42 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-42 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.
		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-42 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-42 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
		• 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.
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 3-39 for more information.
File Name	string	Name of the file.
File Size	uint64	Size of the file in bytes.

Table B-42 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-42 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-42 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.

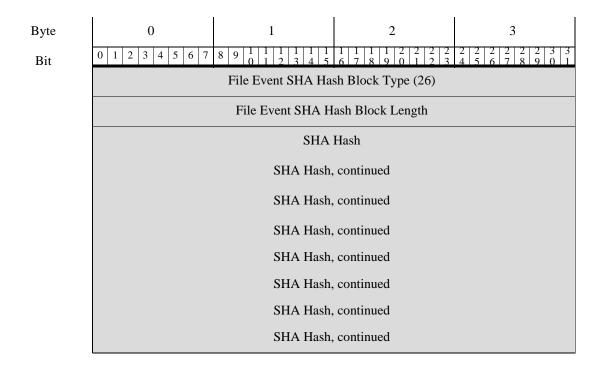
Table B-42 File Event Data Block for 5.4.x Fields (continued)

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 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:



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-43 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-236
- Correlation Event for 5.1-5.3.x, page B-244

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 4-60.

By te	0	1	2	3		
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 1 8 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 V			Type (4)		
		Message	Length			
	Netm	ap ID	Record T	ype (112)		
		Record	Length			
	eStream	ner Server Timestamp ((in events, only if bit 2	3 is set)		
	Reser	ved for Future Use (in	events, only if bit 23 i	s set)		
		Correlation Blo	ock Type (116)			
		Correlation B	Block Length			
		Devic	ce ID			
		(Correlation) l	Event Second			
	Event ID					
	Policy ID					
	Rule ID					
	Priority					
	String Block Type (0)					
		String Blo	ck Length			
		Description		Event Type		
	Event Device ID					
	Signature ID					
	Signature Generator ID					
	(Trigger) Event Second					
	(Trigger) Event Microsecond					
	Event ID Front Defined Mask					
	Event Defined Mask Event Impact Flags IP Protocol Network Protocol					
	Event Impact Flags	IP Protocol	network	FIOLOCOI		

By te	0	1	2	3	
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1	
	Source IP				
	Source Host Type Source VI		LAN ID	Source OS Fprt UUID	Source OS Fprt UUID
		Source OS Fingerpri	nt UUID, continued		
		Source OS Fingerpri	nt UUID, continued		
		Source OS Fingerpri	nt UUID, continued		
	Source O	S Fingerprint UUID, c	ontinued	Source Criticality	
	Source Criticality, cont		Source User ID		
	Source User ID, cont	Source	e Port	Source Server ID	
	Sou	arce Server ID, continu	ed	Destination IP	
	D	estination IP, continue	d	Dest. Host Type	
	Dest. VLAN ID		Destination OS Fingerprint UUID		Dest OS Fingerprint
	1	Destination OS Fingerp	orint UUID, continued		ŬUÎD
	Destination OS Fingerprint UUID, continued				
]	Destination OS Fingerp	orint UUID, continued		
	Destination OS Fi	ingerprint UUID, nued	Destination	Criticality	
		Dest. U	Jser ID		
	Destinat	ion 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	s Interface UUID, cont	inued	Egress Interface UUID	
		Egress Interface U	JUID, continued		

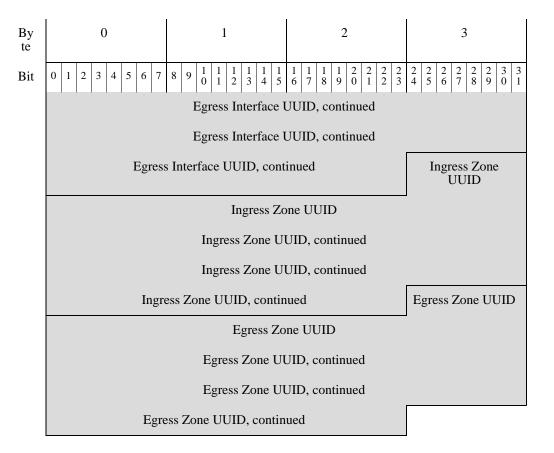


Table B-44 Correlation Event 5.0 - 5.0.2 Data Fields

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 4-60.	
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 3-34 for more information.	
(Correlation) Event Second	uint32	UNIX timestamp indicating the time that the correlation event was generated (in seconds from 01/01/1970).	
Event ID	uint32	Correlation event identification number.	
Policy ID	uint32	Identification number of the correlation policy that was violated. See Server Record, page 4-14 for information about how to obtain policy identification numbers from the database.	
Rule ID	uint32	Identification number of the correlation rule that triggered to violate the policy. See Server Record, page 4-14 for information about how to obtain policy identification numbers from the database.	

Table B-44 Correlation Event 5.0 - 5.0.2 Data Fields (continued)

Field	Data Type	Description
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 4-70.
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 3-34 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 Firepower System preprocessor or rules engine that generated the event.
(Trigger) Event Second	uint32	UNIX timestamp indicating the time of the event that triggered the correlation policy rule (in seconds from 01/01/1970).
(Trigger) Event Microsecond	uint32	Microsecond (one millionth of a second) increment that the event was detected.
Event ID	uint32	Identification number of the event generated by the device.
Event Defined Mask	bits[32]	Set bits in this field indicate which of the fields that follow in the message are valid. See Table B-45 on page B-243 for a list of each bit value.

Table B-44 Correlation Event 5.0 - 5.0.2 Data Fields (continued)

Field	Data Type	Description
Event Impact Flags	bits[8]	Impact flag value of the event. The low-order eight bits indicate the impact level. Values are:
		• 0x01 (bit 0) — Source or destination host is in a network monitored by the system.
		• 0x02 (bit 1) — Source or destination host exists in the network map.
		• 0x04 (bit 2) — Source or destination host is running a server on the port in the event (if TCP or UDP) or uses the IP protocol.
		• 0x08 (bit 3) — There is a vulnerability mapped to the operating system of the source or destination host in the event.
		• 0x10 (bit 4) — There is a vulnerability mapped to the server detected in the event.
		• 0x20 (bit 5) — The event caused the managed device to drop the session (used only when the device is running in inline, switched, or routed deployment). Corresponds to blocked status in the Firepower System web interface.
		• 0x40 (bit 6) — The rule that generated this event contains rule metadata setting the impact flag to red (bit 6). The source or destination host is potentially compromised by a virus, trojan, or other piece of malicious software.
		• 0x80 (bit 7) — There is a vulnerability mapped to the client detected in the event.
		The following impact level values map to specific priorities on the Defense Center. An x indicates the value can be 0 or 1:
		• (0, unknown): 00x00000
		• red (1, vulnerable): xxxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx
		• orange (2, potentially vulnerable): 00x00111
		• yellow (3, currently not vulnerable): 00x00011
		• blue (4, unknown target): 00x00001
IP Protocol	uint8	Identifier of the IP protocol associated with the event, if applicable.
Network Protocol	uint16	Network protocol associated with the event, if applicable.
Source IP	uint8[4]	IP address of the source host in the event, in IP address octets.
Source Host	uint8	Source host's type:
Type		• 0 — Host
		• 1 — Router
		• 2 — Bridge
Source VLAN ID	uint16	Source host's VLAN identification number, if applicable.

Table B-44 Correlation Event 5.0 - 5.0.2 Data Fields (continued)

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

Table B-44 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-45 Event Defined Values

Description	Mask Value
Event Impact Flags	0x0000001
IP Protocol	0x00000002
Network Protocol	0x0000004
Source IP	0x00000008
Source Host Type	0x0000010
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-45 Event Defined Values (continued)

Description	Mask Value
Source User	0x00020000
Destination User	0x00040000

Correlation Event for 5.1-5.3.x

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

You can request 5.1-5.3.x correlation events from eStreamer only by extended request, for which you request event type code 31 and version code 8 in the Stream Request message (see Submitting Extended Requests, page 2-4 for information about submitting extended requests). You can optionally enable bit 23 in the flags field of the initial event stream request message, to include the extended event header. You can also enable bit 20 in the flags field to include user metadata.

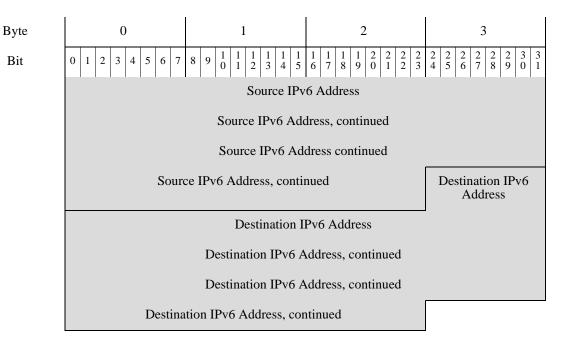
Byte	0	1	2	3	
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 5	1 1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1	
	Header Ve	ersion (1)	Message Type (4)		
	Message Length				
	Netmap ID Record Type (112)			ype (112)	
		Record	Length		
	eStreamer Server Timestamp (in events, only if bit 23 is set)				
	Reserved for Future Use (in events, only if bit 23 is set)				
	Correlation Block Type (128)				
	Correlation Block Length				
	Device ID				
	(Correlation) Event Second				
	Event ID				
	Policy ID				
	Rule ID				
		Prio	rity		

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 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1	
	String Block Type (0)			Event Description
	String Bloo	ck Length		
	Description		Event Type	
	Event De	evice ID		
	Signatu	ıre ID		
	Signature G	enerator ID		
	(Trigger) Ev	rent Second		
	(Trigger) Even	t Microsecond		
	Even	t ID		
	Event Defi	ned 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 Fingerprint 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				
Sou	arce Server ID, continu	ed	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 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 Fingerprint UUID		Dest OS Fingerprint
	Destination OS Finger	print UUID, continued		UUID
	Destination OS Finger	print UUID, continued		
	Destination OS Finger	print UUID, continued		
	Destination OS Fingerprint UUID, continued	Destination	Criticality	
	Dest. U	Jser ID		
	Destination Port	Destination	n 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	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 U	UID, continued		
	Egress Zone UV	UID, continued		
	Egress Zone UUID, contin	ued	Source IPv6 Address	



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 4-60.

Table B-46 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 4-60.
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 3-34 for more information.
(Correlation) Event Second	uint32	UNIX timestamp indicating the time that the correlation event was generated (in seconds from 01/01/1970).
Event ID	uint32	Correlation event identification number.
Policy ID	uint32	Identification number of the correlation policy that was violated. See Server Record, page 4-14 for information about how to obtain policy identification numbers from the database.
Rule ID	uint32	Identification number of the correlation rule that triggered to violate the policy. See Server Record, page 4-14 for information about how to obtain policy identification numbers from the database.
Priority	uint32	Priority assigned to the event. This is an integer value from 0 to 5.

Table B-46 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 4-70.		
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 3-34 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 Firepower 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-45 on page B-243 for a list of each bit value.		

Table B-46 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 Firepower 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			
IP Protocol	uint8	Identifier of the IP protocol associated with the event, if applicable.			
Network Protocol	uint16	Network protocol associated with the event, if applicable.			
Source IP Address	uint8[4]	This field is reserved but no longer populated. The Source IPv4 address is stored in the Source IPv6 Address field. See IP Addresses, page 1-5 for more information.			
Source Host	uint8	Source host's type:			
Type		• 0 — Host			
		• 1 — Router			
		• 2 — Bridge			

Table B-46 Correlation Event 5.1-5.3.x Data Fields (continued)

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

Table B-46 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 2-25 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-252
- Full Host Profile Data Block 5.1.1, page B-261
- Full Host Profile Data Block 5.2.x, page B-269
- Host Profile Data Block for 5.1.x, page B-281
- IP Range Specification Data Block for 5.0 5.1.1.x, page B-287
- Access Control Policy Rule Reason Data Block, page B-287

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 Block Length							
	IP Address							
	Hops	Generic List Block Type (31)						
	Generic List Block Type, continued	Ge	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 ingerprints	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 Fing	gerprint Block Length	
	Operating System Client Fingerprint Data			
	Generic List Block Type (31)			
_	Generic List Block Length			
VDB Native Fingerprints 1	Oŗ	perating System Finger	print Block Type (130)	*
i ingerprints i		Operating System Fing	gerprint Block Length	
		Operating System VD	B Fingerprint Data	
		Generic List B	lock Type (31)	
	Generic List 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)*			
8 1	Operating System Fingerprint Block Length			
	Operating System User Fingerprint Data			
	Generic List Block Type (31)			
,	Generic List Block Length			
Scan Fingerprints	Operating System Fingerprint Block Type (130)*			*
	Operating System Fingerprint Block Length			
	Operating System Scan Fingerprint Data			
	Generic List Block Type (31)			
		Generic List Block Length		

Byte	0 1	2	3
Bit	0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1
Application Fingerprints	Operating System Fingerprint Block Type (130)*		
Tingerprints	Operating System Fingerprint Block Length		
	Operating System Application Fingerprint Data		
	Generic List B	lock Type (31)	
	Generic List Block Length		
Conflict Fingerprints	Operating System Finger	rprint Block Type (130)	*
i ingerprins	Operating System Fin	gerprint Block Length	
	Operating System Con	flict Fingerprint Data	
(TCP) Full Server Data	List Block	Гуре (11)	
	List Block	Length	
	(TCP) Full Server Data Blocks (104)*		
(UDP) Full Server Data	List Block	Type (11)	
	List Block Length		
	(UDP) Full Server Data Blocks (104)*		
Network Protocol Data	List Block Type (11)		
	List Block Length		
	(Network) Protocol Data Blocks (4)*		
Transport Protocol Data	List Block Type (11)		
	List Block Length		
	(Transport) Protocol Data Blocks (4)*		
MAC Address Data	List Block Type (11)		
List Block Length			
	Host MAC Address Data Blocks (95)*		
	Last		
	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 Type, continued Generic List Block Length			Block Length
Dutu	Generic List Block	Length, continued	Full Host Client App (11	plication Data Blocks 2)*
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 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 Bl	ock Type (31)	
	Generic List Block Length			
	(Third Party/VDB) Host Vulnerability Data Blocks (85)*			
3rd Pty Scan Host Vulns	Generic List Block Type (31)			
	Generic List Block Length			
	(Third Party Scan) Host Vulnerability Data Blocks with Original Vuln IDs (85)*			
Attribute Value Data		List Block		
	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-47 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-47 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 4-156 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 4-156 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 4-156 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-47 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 4-156 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 4-156 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 4-156 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 4-156 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-47 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 4-156 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 4-156 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 4-137 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 4-137 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 4-74 for a description of this data block.	

Table B-47 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 4-74 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 4-113 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 4-151 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-47 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 4-110 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 4-110 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 4-110 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 4-80 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 1 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1
		Full Host Profile	Data Block (135)	
	Data Block Length			
		IP Ac	ldress	
	Hops	Ge	neric List Block Type	(31)
	Generic List Block Type, continued	G	eneric List Block Leng	gth
OS Derived Fingerprints	Generic List Block Length, continued	OS Fingerprint Operating System Fingerprint Block Length con't		k Type (130)*
	OS Fingerprint Block Type (130)*, con't			ock Length
	OS Fingerprint Block Length, con't			print Data
	Generic List Block Type (31)			
	Generic List Block Length			
Server Fingerprints	Operating System Fingerprint Block Type (130)*			
1 mgerprims	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 1 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)*			
1 mgorprimos	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 Fingerprint Block Length			
	Operating System Application Fingerprint Data			
	Generic List Block Type (31)			
	Generic List Block Length			
Conflict Fingerprints	Operating System Finger	rprint Block Type (130)*		
Tingerprints	Operating System Fin	gerprint Block Length		
	Operating System Con	flict 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			
	(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 5	1 1 1 1 2 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1	
	VLAN Type	VLAN Priority	Generic List B	lock Type (31)	
Host Client Data	Generic List Block Type, continued Generic List Block Length				
Butt	Generic List Block	Length, continued	Full Host Client App (11	lication Data Blocks 2)*	
NetBIOS Name		String Bloc	k Type (0)		
		String Blo	ck Length		
		NetBIOS Na	ame String		
Notes Data		String Bloc	k Type (0)		
	String Block Length				
		Notes S	tring		
(VDB) Host Vulns	Generic List Block Type (31)				
, 2222	Generic List Block Length				
	(VDB) Host Vulnerability Data Blocks (85)*				
3rd Pty/VDB) Host Vulns	Generic List Block Type (31)				
	Generic List Block Length				
	(Third Party/VDB) Host Vulnerability Data Blocks (85)*				
3rd Pty Scan Host Vulns		Generic List B	lock Type (31)		
11000 (01110	Generic List 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				
, and Batta					
	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-48 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 4-156 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 4-156 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 4-156 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 4-156 for a description of this data block.	

Table B-48 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 4-156 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 4-156 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 4-156 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 4-156 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-48 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 4-156 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 4-137 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 4-137 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 4-74 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 4-74 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-48 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 4-113 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 4-151 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-48 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 4-110 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 4-110 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 4-110 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 4-80 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 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
	Full Host Profile Data Block (140)			
	Data Block Length			
		Hos	st ID	
		Host ID,	continued	
		Host ID,	continued	
		Host ID,	continued	
IP Addresses		List Block	Type (11)	
		List Bloo	ck Length	
		IP Address Dat	a Blocks (143)*	
	Hops	Ge.	neric List Block Type (3	31)
	Generic List Block Type, continued Generic List Block Length		h	
OS Derived Fingerprints	Generic List Block Length, continued Operating System Fingerprint Block Type (130)*			Type (130)*
	OS Fingerprint Block Type (130)*, con't	Operating	System Fingerprint Bloo	ck Length
	OS Fingerprint Block Length, con't	Operating S	System Derived Fingerp	rint Data
		Generic List B	slock Type (31)	
		Generic List	Block Length	
Server Fingerprints	Operating System Fingerprint Block Type (130)*		*	
6 · F	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)*			
i ingerprints	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)*			
	Operating System Fingerprint Block Length			
	Operating System VDB Fingerprint Data			
	Generic List Block Type (31)			
	Generic List Block Length			
VDB Native Fingerprints 2	Operating System Fingerprint Block Type (130)*			
	Operating System Fingerprint Block Length			
	Operating System VDB Fingerprint Data			
	Generic List Block Type (31)			
	Generic List Block Length			
User Fingerprints	Operating System Fingerprint Block Type (130)*			
	Operating System Fingerprint Block Length			
	Operating System User Fingerprint Data			
	Generic List Block Type (31)			
	Generic List Block Length			
Scan Fingerprints	Operating System Fingerprint Block Type (130)*			
	Operating System Fingerprint Block Length			
	Operating System Scan Fingerprint Data			
	Generic List Block Type (31)			
	Generic List Block Length			

Byte	0	1	2	3	
Bit	0 1 2 3 4 5 6 7	8 9 1 1 1 1 1 1 1 1 5		2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1	
Application Fingerprints	Operating System Fingerprint Block Type (130)*				
Tingerprints	Operating System Fingerprint Block Length				
	Oj	perating System Appli	cation Fingerprint Data	a	
		Generic List F	Block Type (31)		
		Generic List	Block Length		
Conflict Fingerprints	Ol	perating System Finge	erprint Block Type (130))*	
1 mgupimus		Operating System Fir	ngerprint Block Length		
	(Operating System Cor	nflict Fingerprint Data		
		Generic List E	Block Type (31)		
		Generic List	Block Length		
Mobile Fingerprints	Oj	perating System Finge	erprint Block Type (130))*	
	Operating System Fingerprint Block Length				
	Operating System Mobile Fingerprint Data				
	Generic List Block Type (31)				
		Generic List	Block Length		
IPv6 Server Fingerprints	Ol	perating System Finge	erprint Block Type (130))*	
		Operating System Fir	ngerprint Block Length		
	Ol	perating System IPv6	Server Fingerprint Data	a	
		Generic List F	Block Type (31)		
		Generic List	Block Length		
Ipv6 Client Fingerprints	Operating System Fingerprint Block Type (130)*				
		Operating System Fir	ngerprint Block Length		
	Operating System Ipv6 Client Fingerprint Data			ı	
	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)*				
ringerprints	Operating System Fingerprint 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)*			
1 ingerprints	Operating System Fin	gerprint Block Length			
	Operating System User A	Agent Fingerprint Data			
(TCP) Full Server Data	List Block	Type (11)			
Server Buttur	List Block	c Length			
	(TCP) Full Server	(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) Protoco	ol Data Blocks (4)*			
Transport Protocol Data	List Block Type (11)				
	List Block Length				
	(Transport) Protocol Data Blocks (4)*				
MAC Address Data	Type (11)				
	List Block Length				
	Host MAC Address Data Blocks (95)*				
		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 B	lock Type (31)	
Host Client Data	Generic List Block Type, continued Generic List Block Length				
Dutu	Generic List Block	Length, continued	Full Host Client App (11)		
NetBios Name		String Bloc	k Type (0)		
Name		String Blo	ck Length		
		NetBIOS Na	ame String		
Notes Data		String Bloc	k Type (0)		
		String Blo	ck Length		
	Notes String				
(VDB) Host Vulns	Generic List Block Type (31)				
, 5555	Generic List Block Length				
		(VDB) Host Vulnerabi	lity Data Blocks (85)*		
3rd Pty/VDB) Host Vulns	Generic List Block Type (31)				
	Generic List Block Length				
	(Third	Party/VDB) Host Vul	nerability Data Blocks	(85)*	
3rd Pty Scan Host Vulns		Generic List B	lock Type (31)		
11000 (01110		Generic List l	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-49 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 4-95 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 4-156 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 4-156 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 4-156 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-49 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 4-156 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 4-156 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 4-156 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 4-156 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-49 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 4-156 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 4-156 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 4-156 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 4-156 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-49 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 4-156 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 4-156 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 4-156 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 4-137 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 4-137 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-49 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 4-74 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 4-74 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 4-113 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-49 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 4-151 for a description of this data block.	
String Block Type	uint32	Initiates a String data block for the host NetBIOS name. This value is always 0.	
String Block Length	uint32	Number of bytes in the String data block, including eight bytes for the string block type and length fields, plus the number of bytes in the NetBIOS name string.	
NetBIOS Name	string	Host NetBIOS name string.	
String Block Type	uint32	Initiates a String data block for host notes. This value is always 0.	
String Block Length	uint32	Number of bytes in the notes String data block, including eight bytes for the string block type and length fields, plus the number of bytes in the notes string.	
Notes	string	Contains the contents of the Notes host attribute for the host.	
Generic List Block Type	uint32	Initiates a Generic List data block comprising Host Vulnerability data blocks conveying VDB vulnerability data. This value is always 31.	
Generic List Block Length	uint32	Number of bytes in the Generic List data block, including the list header and all encapsulated data blocks.	
(VDB) Host Vulnerability Data Blocks *	variable	List of Host Vulnerability data blocks for vulnerabilities identified in the Cisco vulnerability database (VDB). See Host Vulnerability Data Block 4.9.0+, page 4-110 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 4-110 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 4-110 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-49 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 4-80 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 Blo	ock Type (132)		
		Host Profile I	Block Length		
		IP Ad	dress		
Server Fingerprints	Hops	Primary/Secondary	Generic List B	lock Type (31)	
1 mgorprints	Generic List Block Type, continued Generic			Block Length	
	Generic List Block Length, continued Server Fingerprint Data Blocks*			nt Data Blocks*	
Client Fingerprints	Generic List Block Type (31)				
1 mgv.pmms	Generic List Block Length				
	Client Fingerprint Data Blocks*				
SMB Fingerprints	Generic List Block Type (31)				
- ingerprints	Generic List Block Length				
	SMB Fingerprint Data Blocks*				

Byte	0	1	2	3		
Bit	0 1 2 3 4 5 6 7					
DHCP Fingerprints		Generic List Block Type (31)				
ringerprints		Generic List	Block Length			
		DHCP Fingerpr	int Data Blocks*			
Mobile Device		Generic List B	Block Type (31)			
Fingerprints		Generic List	Block Length			
		Mobile Device Fing	erprint Data Blocks*			
TCP Server Block*		List Block	Type (11)		List of TCP Servers	
Brock		List Bloo	ck Length		Servers	
		TCP Server	Data Blocks			
UDP Server Block*	List Block Type (11)				List of UDP Servers	
		UDP Server	Data Blocks			
Network Protocol	List Block Type (11)				List of Network Protocols	
Block*						
Transport Protocol	List Block Type (11)			List of Transport		
Block*		List Block Length				
		Transport Proto	ocol Data Blocks			
MAC Address Block*		List Block	Type (11)		List of MAC Addresses	
	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 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	String Block Type (0)				
rvanie	String Block Length				
	NetBIOS String Data				

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

Table B-50 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 4-156 for a description of this data block.	

Table B-50 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 4-156 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 4-156 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 4-156 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-50 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 4-156 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 4-74 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 4-74 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.	

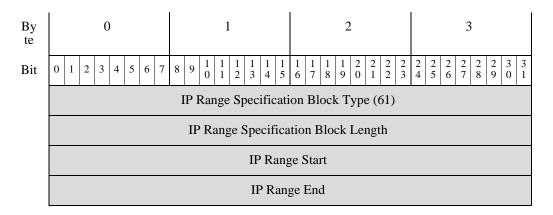
Table B-50 Host Profile Data Block 5.1.x Fields (continued)

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 4-113 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 4-151 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-51 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 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 Policy Rule Reason Data Block Type (21)				
	Access Control Policy Rule Reason Data Block Length				
Description	Rea	son	String Block Type (0)		
	String Block Typ	e (0), continued	String Block Length		
	String Block Le	ngth, continued	Description		

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

Table B-52 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.