Understanding Host Data Structures

This chapter describes the format of the Full Host Profile data block that conveys a set of data describing a single host. The eStreamer server generates and sends these blocks on request for host data. For information about the client request procedure, the message structure, and the delivery method, see Host Data and Multiple Host Data Message Format, page 2-30.

eStreamer uses the series 1 data block structure to package these Full Host profile blocks. For the general structure of series 1 blocks, see Series 1 Data Block Header, page 4-61. The Full Host Profile data block contains a number of encapsulated blocks which are individually described in the subsections where they are defined in Understanding Discovery & Connection Data Structures, page 4-1.

See the following sections for more information about current and legacy Full Host Profile data blocks:

- Full Host Profile Data Block 5.3+, page 5-1 describes the current Full Host Profile data block structure.
- Full Host Profile Data Block 5.0 - 5.0.2, page B-269 describes the legacy Full Host Profile data block structure for versions 5.0 - 5.0.2.

Full Host Profile Data Block 5.3+

The Full Host Profile data block for version 5.3+ 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 149. It supersedes the prior version, which has a block type of 140.

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

The following diagram shows the format of the Full Host Profile data block for 5.3+:

Byte	0								1								2								3							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	Full Host Profile Data Block (149)																															
	Data Block Length																															
	Host ID Host ID, continued Host ID, continued Host ID, continued																															
IP Addresses	List Block Type (11)																															
	List Block Length																															
	IP Address Data Blocks (143)*																															
	Hops								Generic List Block Type (31)																							
	Generic List Block Type, continued								Generic List Block Length																							
OS Derived Fingerprints	Generic List Block Length, continued								Operating System Fingerprint Block Type (130)*																							
	OS Fingerprint Block Type (130)*, con't								Operating System Fingerprint Block Length																							
	OS Fingerprint Block Length, con't								Operating System Derived Fingerprint Data...																							
	Generic List Block Type (31)																															
	Generic List Block Length																															
Server Fingerprints	Operating System Fingerprint Block Type (130)*																															
	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	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Client Fingerprints	Operating System Fingerprint Block Type (130)*																															
	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	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Application Fingerprints	Operating System Fingerprint Block Type (130)*																															
	Operating System Fingerprint Block Length																															
	Operating System Application Fingerprint Data...																															
	Generic List Block Type (31)																															
	Generic List Block Length																															
Conflict Fingerprints	Operating System Fingerprint Block Type (130)*																															
	Operating System Fingerprint Block Length																															
	Operating System Conflict Fingerprint Data...																															
	Generic List Block Type (31)																															
	Generic List Block Length																															
Mobile Fingerprints	Operating System Fingerprint 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	Operating System Fingerprint Block Type (130)*																															
	Operating System Fingerprint Block Length																															
	Operating System IPv6 Server Fingerprint Data...																															
	Generic List Block Type (31)																															
	Generic List Block Length																															
Ipv6 Client Fingerprints	Operating System Fingerprint Block Type (130)*																															
	Operating System Fingerprint Block Length																															
	Operating System Ipv6 Client Fingerprint Data...																															
	Generic List Block Type (31)																															
	Generic List Block Length																															

Byte	0								1								2								3							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Ipv6 DHCP Fingerprints	Operating System Fingerprint Block Type (130)*																															
	Operating System Fingerprint Block Length																															
	Operating System IPv6 DHCP Fingerprint Data...																															
	Generic List Block Type (31)																															
	Generic List Block Length																															
User Agent Fingerprints	Operating System Fingerprint Block Type (130)*																															
	Operating System Fingerprint Block Length																															
	Operating System User Agent Fingerprint Data...																															
(TCP) Full Server Data	List Block Type (11)...																															
	List Block Length...																															
	(TCP) Full Server Data Blocks (104)*																															
(UDP) Full Server Data	List Block Type (11)																															
	List Block Length																															
	(UDP) Full Server Data Blocks (104)*																															
Network Protocol Data	List Block Type (11)																															
	List Block Length																															
	(Network) Protocol Data Blocks (4)*																															
Transport Protocol Data	List Block Type (11)																															
	List Block Length																															
	(Transport) Protocol Data Blocks (4)*																															
MAC Address Data	List Block Type (11)																															
	List Block Length																															
	Host MAC Address Data Blocks (95)*																															
	Last Seen																															
	Host Type																															
	Business Criticality																VLAN ID															

Byte	0								1								2								3							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	VLAN Type								VLAN Priority								Generic List Block Type (31)															
Host Client Data	Generic List Block Type, continued																Generic List Block Length															
	Generic List Block Length, continued																Full Host Client Application Data Blocks (112)*															
NetBios Name	String Block Type (0)																															
Name	String Block Length																															
	NetBIOS Name String...																															
Notes Data	String Block Type (0)																															
	String Block Length																															
	Notes String....																															
(VDB) Host Vulns	Generic List Block Type (31)																															
	Generic List Block Length																															
	(VDB) Host Vulnerability Data Blocks (85)*																															
3rd Pty/VDB) Host Vulns	Generic List Block Type (31)																															
	Generic List Block Length																															
	(Third Party/VDB) Host Vulnerability Data Blocks (85)*																															
3rd Pty Scan Host Vulns	Generic List Block Type (31)																															
	Generic List Block Length																															
	(Third Party Scan) Host Vulnerability Data Blocks with Original Vuln IDs (85)*																															
Attribute Value Data	List Block Type (11)																															
	List Block Length																															
	Attribute Value Data Blocks *																															
	Mobile								Jailbroken								Generic List Block Type (31)															
IOC State	Generic List Block Type, continued																Generic List Block Length															
	Generic List Block Length, continued																IOC State Data Blocks (150)*															

The following table describes the components of the Full Host Profile for 5.3+ record.

Table 5-1 Full Host Profile Record 5.3+ 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 5-1 Full Host Profile Record 5.3+ 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 5-1 Full Host Profile Record 5.3+ 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 5-1 Full Host Profile Record 5.3+ 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 4-136 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 4-136 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 5-1 Full Host Profile Record 5.3+ 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 5-1 Full Host Profile Record 5.3+ 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 5-1 Full Host Profile Record 5.3+ 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.
Generic List Block Type	uint32	Initiates a Generic List data block comprising IOC State data blocks.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 IOC State data blocks.
IOC State Data Blocks *	variable	IOC State data blocks containing information about compromises on a host. See IOC State Data Block for 5.3+, page 4-33 for a description of this data block.