



Version 6.6
November 10, 2020 i

Introduction 1-1

- Major Changes in eStreamer Version 6.6 1-1
- Using this Guide 1-1
- Prerequisites 1-2
- Product Versions for Firepower System Releases 1-2
- Document Conventions 1-3
 - IP Addresses 1-4
- Best Practices 1-4

Understanding the eStreamer Application Protocol 2-1

- Connection Specifications 2-1
- Understanding eStreamer Communication Stages 2-2
 - Establishing an Authenticated Connection 2-2
 - Requesting Data from eStreamer 2-3
 - Establishing a Session 2-3
 - Using Event Stream Requests and Extended Requests to Initiate Event Streaming 2-3
 - Submitting Event Stream Requests 2-4
 - Submitting Extended Requests 2-4
 - Requesting Host Data 2-4
 - Changing a Request 2-5
- Accepting Data from eStreamer 2-5
 - Event Stream Requests 2-5
 - Extended Requests 2-5
- Terminating Connections 2-5
- Understanding eStreamer Message Types 2-6
 - eStreamer Message Header 2-7
- Null Message Format 2-7
- Error Message Format 2-8
- Event Stream Request Message Format 2-10
 - Initial Timestamp 2-11

- Request Flags 2-11
- Event Data Message Format 2-17
 - Understanding the Organization of Event Data Messages 2-17
 - Intrusion Event and Metadata Message Format 2-18
 - Discovery Event Message Format 2-19
 - Discovery Event Message Headers 2-20
 - Connection Event Message Format 2-21
 - Correlation Event Message Format 2-21
 - Correlation Record Header 2-21
 - Event Extra Data Message Format 2-23
 - Event Extra Data Message Record Header 2-23
 - Data Block Header 2-24
- Host Request Message Format 2-25
- Rule Documentation Message Format 2-29
- Host Data and Multiple Host Data Message Format 2-30
- Streaming Information Message Format 2-31
- Streaming Request Message Format 2-32
- Streaming Service Request Structure 2-33
 - 2-34
- Domain Streaming Request Message Format 2-34
- Streaming Event Type Structure 2-35
- Sample Extended Request Messages 2-38
 - Streaming Information Message 2-38
 - Streaming Request Message 2-38
- Message Bundle Format 2-39
- Understanding Metadata 2-40
 - Metadata Transmission 2-40
- Understanding Intrusion and Correlation Data Structures 3-1**
 - Intrusion Event and Metadata Record Types 3-1
 - Packet Record 4.8.0.2+ 3-5
 - Priority Record 3-6
 - Intrusion Event Record 6.0+ 3-7
 - Intrusion Impact Alert Data 5.3+ 3-16
 - User Record 3-19
 - Rule Message Record for 4.6.1+ 3-20
 - Classification Record for 4.6.1+ 3-21
 - Correlation Policy Record 3-22

Correlation Rule Record	3-24
Intrusion Event Extra Data Record	3-25
Intrusion Event Extra Data Metadata	3-27
Security Zone Name Record	3-28
Interface Name Record	3-30
Access Control Policy Name Record	3-31
Access Control Rule ID Record Metadata	3-32
Managed Device Record Metadata	3-34
Malware Event Record 5.1.1+	3-34
Cisco Advanced Malware Protection Cloud Name Metadata	3-35
Malware Event Type Metadata	3-37
Malware Event Subtype Metadata	3-38
AMP for Endpoints Detector Type Metadata	3-38
AMP for Endpoints File Type Metadata	3-39
Security Context Name	3-40
Correlation Event for 5.4+	3-41
Understanding Series 2 Data Blocks	3-54
Series 2 Primitive Data Blocks	3-57
String Data Block	3-57
BLOB Data Block	3-58
List Data Block	3-59
Generic List Data Block	3-60
UUID String Mapping Data Block	3-60
Name Description Mapping Data Block	3-61
Access Control Policy Rule ID Metadata Block	3-63
ICMP Type Data Block	3-64
ICMP Code Data Block	3-65
Security Intelligence Category Metadata for 5.4.1+	3-66
Realm Metadata for 6.0+	3-67
Endpoint Profile Data Block for 6.0+	3-68
Security Group Metadata for 6.0+	3-69
DNS Record Type Metadata for 6.0+	3-70
DNS Response Type Metadata for 6.0+	3-72
Sinkhole Metadata for 6.0+	3-73
Netmap Domain Metadata for 6.0+	3-74
Access Control Policy Rule Reason Data Block for 6.0+	3-75
Access Control Policy Name Data Block	3-77
IP Reputation Category Data Block	3-78
File Event for 6.0+	3-79
Malware Event Data Block 6.0+	3-89

- File Event SHA Hash for 5.3+ 3-99
- File Type ID Metadata for 5.3+ 3-101
- Rule Documentation Data Block for 5.2+ 3-102
- Filelog Storage Metadata for 6.0+ 3-106
- Filelog Sandbox Metadata for 6.0+ 3-106
- Filelog Spero Metadata for 6.0+ 3-107
- Filelog Archive Metadata for 6.0+ 3-108
- Filelog Static Analysis Metadata for 6.0+ 3-109
- Geolocation Data Block for 5.2+ 3-109
- File Policy Name for 6.0+ 3-110
- SSL Policy Name 3-112
- SSL Rule ID 3-113
- SSL Cipher Suite 3-114
- SSL Version 3-115
- SSL Server Certificate Status 3-116
- SSL Actual Action 3-116
- SSL Expected Action 3-117
- SSL Flow Status 3-118
- SSL URL Category 3-119
- SSL Certificate Details Data Block for 5.4+ 3-120
- Network Analysis Policy Name Record 3-124

Understanding Discovery & Connection Data Structures 4-1

- Discovery and Connection Event Data Messages 4-2
 - Discovery and Connection Event Record Types 4-2
- Metadata for Discovery Events 4-7
 - Fingerprint Record 4-7
 - Client Application Record 4-9
 - Vulnerability Record 4-9
 - Criticality Record 4-12
 - Network Protocol Record 4-12
 - Attribute Record 4-13
 - Scan Type Record 4-14
 - Service Record 4-15
 - Source Type Record 4-16
 - Source Application Record 4-16
 - Source Detector Record 4-17
 - Third Party Scanner Vulnerability Record 4-18
 - User Record 4-19

Web Application Record	4-21
Intrusion Policy Name Record	4-22
Access Control Rule Action Record Metadata	4-23
URL Category Record Metadata	4-24
URL Reputation Record Metadata	4-24
Access Control Rule Reason Metadata	4-25
Access Control Policy Metadata	4-27
Prefilter Policy Metadata	4-29
Tunnel or Prefilter Rule Metadata	4-30
Security Intelligence Category Metadata	4-32
Security Intelligence Source/Destination Record	4-33
IOC State Data Block for 5.3+	4-34
IOC Name Data Block for 5.3+	4-36
Discovery Event Header 5.2+	4-40
Discovery and Connection Event Types and Subtypes	4-42
Host Discovery Structures by Event Type	4-44
New Host and Host Last Seen Messages	4-45
Server Messages	4-46
New Network Protocol Message	4-47
New Transport Protocol Message	4-47
Client Application Messages	4-47
IP Address Change Message	4-48
Operating System Update Messages	4-49
IP Address Reused and Host Timeout/Deleted Messages	4-49
Hops Change Message	4-50
TCP and UDP Port Closed/Timeout Messages	4-50
MAC Address Messages	4-51
Host Identified as a Bridge/Router Message	4-51
VLAN Tag Information Update Messages	4-52
Change NetBIOS Name Message	4-52
Update Banner Message	4-53
Policy Control Message	4-53
Connection Statistics Data Message	4-53
Connection Chunk Message	4-54
User Set Vulnerabilities Messages for Version 4.6.1+	4-54
User Add and Delete Host Messages	4-55
User Delete Server Message	4-55
User Set Host Criticality Messages	4-56
Attribute Messages	4-56
Attribute Value Messages	4-57

- User Server and Operating System Messages 4-57
 - User Protocol Messages 4-58
 - User Client Application Messages 4-58
 - Add Scan Result Messages 4-59
 - New Operating System Messages 4-59
- Identity Conflict and Identity Timeout System Messages 4-60
- Host IOC Set Messages 4-60
- User Data Structures by Event Type 4-61
 - User Modification Messages 4-61
 - User Information Update Message Block 4-62
- Understanding Discovery (Series 1) Blocks 4-62
 - Series 1 Data Block Header 4-62
 - Series 1 Primitive Data Blocks 4-63
- Host Discovery and Connection Data Blocks 4-63
 - String Data Block 4-71
 - BLOB Data Block 4-72
 - List Data Block 4-72
 - Generic List Block 4-73
 - Sub-Server Data Block 4-74
 - Protocol Data Block 4-75
 - Integer (INT32) Data Block 4-76
 - VLAN Data Block 4-76
 - Server Banner Data Block 4-77
 - String Information Data Block 4-78
 - Attribute Address Data Block 5.2+ 4-79
 - User IOC Change Data Block 5.3+ 4-80
 - Attribute List Item Data Block 4-81
 - Attribute Value Data Block 4-82
 - Full Sub-Server Data Block 4-84
 - Operating System Data Block 3.5+ 4-86
 - Policy Engine Control Message Data Block 4-86
 - Attribute Definition Data Block for 4.7+ 4-87
 - User Protocol Data Block 4-90
 - User Client Application Data Block for 5.1.1+ 4-92
 - User Client Application List Data Block 4-93
 - IP Address Range Data Block for 5.2+ 4-95
 - Attribute Specification Data Block 4-96
 - Host IP Address Data Block 4-97
 - MAC Address Specification Data Block 4-98
 - Address Specification Data Block 4-99

Connection Chunk Data Block for 6.1+	4-100
Fix List Data Block	4-102
User Server Data Block	4-102
User Server List Data Block	4-104
User Hosts Data Block 4.7+	4-105
User Vulnerability Change Data Block 4.7+	4-106
User Criticality Change Data Block 4.7+	4-108
User Attribute Value Data Block 4.7+	4-109
User Protocol List Data Block 4.7+	4-111
Host Vulnerability Data Block 4.9.0+	4-112
Identity Data Block	4-113
Host MAC Address 4.9+	4-115
Secondary Host Update	4-116
Web Application Data Block for 5.0+	4-117
Connection Statistics Data Block 6.2+	4-118
Scan Result Data Block 5.2+	4-134
Host Server Data Block 4.10.0+	4-136
Full Host Server Data Block 4.10.0+	4-138
Server Information Data Block for 4.10.x, 5.0 - 5.0.2	4-142
Full Server Information Data Block	4-144
Generic Scan Results Data Block for 4.10.0+	4-147
Scan Vulnerability Data Block for 4.10.0+	4-149
Full Host Client Application Data Block 5.0+	4-152
Host Client Application Data Block for 5.0+	4-153
User Vulnerability Data Block 5.0+	4-155
Operating System Fingerprint Data Block 5.1+	4-157
Mobile Device Information Data Block for 5.1+	4-159
Host Profile Data Block for 5.2+	4-160
User Product Data Block 5.1+	4-168
User Data Blocks	4-174
User Account Update Message Data Block	4-176
User Information Data Block for 6.0+	4-185
VPN Session Data Block for 6.2+	4-188
User Login Information Data Block 6.2+	4-190
Discovery and Connection Event Series 2 Data Blocks	4-194
Access Control Rule Data Block	4-195
Access Control Rule Reason Data Block 5.1+	4-196
Security Intelligence Category Data Block 5.1+	4-198
User Data Block	4-199
Access Control Policy Metadata Block 6.0+	4-200

Understanding Host Data Structures 5-1

Full Host Profile Data Block 5.3+ 5-1

Configuring eStreamer 6-1

Configuring eStreamer on the eStreamer Server 6-1

Configuring eStreamer Event Types 6-2

Adding Authentication for eStreamer Clients 6-3

Managing the eStreamer Service 6-4

Starting and Stopping the eStreamer Service 6-4

eStreamer Service Options 6-4

Running the eStreamer Service in Debug Mode 6-5

Configuring the eStreamer Reference Client 6-6

Setting Up the eStreamer Perl Reference Client 6-6

Understanding the eStreamer Perl Reference Client 6-6

Configuring Communications for the eStreamer Reference Client 6-7

Loading General Prerequisites for the Perl Reference Client 6-7

Loading Prerequisites for the Perl SNMP Reference Client 6-7

Understanding the Data Requested by a Test Script 6-8

Modifying the Type of Data Requested by a Test Script 6-9

Creating a Certificate for the Perl Reference Client 6-10

Running the eStreamer Perl Reference Client 6-11

Testing a Client Connection over SSL Using a Host Request 6-11

Capturing a PCAP Using the Reference Client 6-11

Capturing CSV Records Using the Reference Client 6-12

Sending Records to an SNMP Server Using the Reference Client 6-12

Logging Events to the Syslog Using the Reference Client 6-12

Connecting to an IPv6 Address 6-12

Data Structure Examples A-1

Intrusion Event Data Structure Examples A-1

Example of an Intrusion Event for the Management Center 5.4+ A-1

Example of an Intrusion Impact Alert A-6

Example of a Packet Record A-8

Example of a Classification Record A-9

Example of a Priority Record A-11

Example of a Rule Message Record A-12

Example of a Connection Statistics Data Block for 6.1.x A-14

Example of a Version 5.1+ User Event A-27

Discovery Data Structure Examples A-30

Example of a New Network Protocol Message A-30

Example of a New TCP Server Message **A-31**

Understanding Legacy Data Structures B-1

Legacy Intrusion Data Structures **B-1**

Intrusion Event (IPv4) Record 5.0.x - 5.1 **B-2**

Intrusion Event (IPv6) Record 5.0.x - 5.1 **B-6**

Intrusion Event Record 5.2.x **B-12**

Intrusion Event Record 5.3 **B-17**

Intrusion Event Record 5.1.1.x **B-23**

Intrusion Event Record 5.3.1 **B-29**

Intrusion Event Record 5.4.x **B-36**

Intrusion Impact Alert Data **B-44**

Legacy Malware Event Data Structures **B-46**

Malware Event Data Block 5.1 **B-46**

Malware Event Data Block 5.1.1.x **B-50**

Malware Event Data Block 5.2.x **B-56**

Malware Event Data Block 5.3 **B-63**

Malware Event Data Block 5.3.1 **B-70**

Malware Event Data Block 5.4.x **B-77**

Legacy Discovery Data Structures **B-87**

Legacy Discovery Event Header **B-87**

Discovery Event Header 5.0 - 5.1.1.x **B-87**

Legacy Server Data Blocks **B-89**

Attribute Address Data Block for 5.0 - 5.1.1.x **B-89**

Legacy Client Application Data Blocks **B-90**

User Client Application Data Block for 5.0 - 5.1 **B-90**

Legacy Scan Result Data Blocks **B-91**

Scan Result Data Block 5.0 - 5.1.1.x **B-92**

User Product Data Block for 5.0.x **B-94**

Legacy User Login Data Blocks **B-100**

User Login Information Data Block for 5.0 - 5.0.2 **B-100**

User Login Information Data Block 5.1-5.4.x **B-102**

User Login Information Data Block 6.0.x **B-104**

User Login Information Data Block 6.1.x **B-107**

B-109

User Login Information Data Block 6.1.x **B-110**

User Information Data Block for 5.x **B-114**

Legacy Host Profile Data Blocks **B-116**

Host Profile Data Block for 5.0 - 5.0.2 **B-116**

Legacy OS Fingerprint Data Blocks **B-123**

Operating System Fingerprint Data Block for 5.0 - 5.0.2	B-123
Legacy Connection Data Structures	B-124
Connection Statistics Data Block 5.0 - 5.0.2	B-125
Connection Statistics Data Block 5.1	B-129
Connection Statistics Data Block 5.2.x	B-135
Connection Chunk Data Block for 5.0 - 5.1	B-141
Connection Chunk Data Block for 5.1.1-6.0.x	B-142
Connection Statistics Data Block 5.1.1.x	B-144
Connection Statistics Data Block 5.3	B-150
Connection Statistics Data Block 5.3.1	B-156
Connection Statistics Data Block 5.4	B-163
Connection Statistics Data Block 5.4.1	B-176
Connection Statistics Data Block 6.0.x	B-189
Connection Statistics Data Block 6.1.x	B-204
Legacy File Event Data Structures	B-221
File Event for 5.1.1.x	B-221
File Event for 5.2.x	B-225
File Event for 5.3	B-229
File Event for 5.3.1	B-235
File Event for 5.4.x	B-241
File Event SHA Hash for 5.1.1-5.2.x	B-251
Legacy Correlation Event Data Structures	B-252
Correlation Event for 5.0 - 5.0.2	B-252
Correlation Event for 5.1-5.3.x	B-260
Legacy Host Data Structures	B-267
Full Host Profile Data Block 5.0 - 5.0.2	B-268
Full Host Profile Data Block 5.1.1	B-277
Full Host Profile Data Block 5.2.x	B-285
Host Profile Data Block for 5.1.x	B-297
IP Range Specification Data Block for 5.0 - 5.1.1.x	B-303
Access Control Policy Rule Reason Data Block	B-303