Data Sample

Sample Log Field Names & Types

FortiGate East-Aus 7121F		
Field Names	**Field Type**	**Regex**
src-ip	IPv4	^(?:[0-9]{1,3}\.){3}[0-9]{1,3}$
scr-ip6	IPv6	(([0-9a-fA-F]{1,4}:){7,7}[0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}:){1,7}:|([0-9a-fA-F]{1,4}:){1,6}:[0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}:){1,5}(:[0-9a-fA-F]{1,4}){1,2}|([0-9a-fA-F]{1,4}:){1,4}(:[0-9a-fA-F]{1,4}){1,3}|([0-9a-fA-F]{1,4}:){1,3}(:[0-9a-fA-F]{1,4}){1,4}|([0-9a-fA-F]{1,4}:){1,2}(:[0-9a-fA-F]{1,4}){1,5}|[0-9a-fA-F]{1,4}:((:[0-9a-fA-F]{1,4}){1,6})|:((:[0-9a-fA-F]{1,4}){1,7}|:)|fe80:(:[0-9a-fA-F]{0,4}){0,4}%[0-9a-zA-Z]{1,}|::(ffff(:0{1,4}){0,1}:){0,1}((25[0-5]|(2[0-4]|1{0,1}[0-9]){0,1}[0-9])\.){3,3}(25[0-5]|(2[0-4]|1{0,1}[0-9]){0,1}[0-9])|([0-9a-fA-F]{1,4}:){1,4}:((25[0-5]|(2[0-4]|1{0,1}[0-9]){0,1}[0-9])\.){3,3}(25[0-5]|(2[0-4]|1{0,1}[0-9]){0,1}[0-9]))
src-port	port	
id	device-id	\d{7,}
time	UTC	\d{4}-(?:0[1-9]|1[0-2])-(?:0[1-9]|[1-2]\d|3[0-1])T(?:[0-1]\d|2[0-3]):[0-5]\d:[0-5]\d
message	Message	*
mac-addr	MAC	^([0-9A-Fa-f]{2}[:-]){5}([0-9A-Fa-f]{2})$

Input Device Names ***Source From Cisco Products List***	
Firepower 1140	Catalyst C3560CX-8PC
Firepower 1150	MS210-24
Firepower 4112	MS250-24P
Firepower 4145	Nexus 9332D-GX2B
Catalyst C3560CX-12PC	Nexus 9500 X9716-GX

Input Device Names ***Source From Fortinet Products***	
FortiGate 7121F	FortiAnalyzer 3700F
FortiADC 400D	FortiGate 3980E
FortiADC 200F	FortiGate 3400E
FortiAnalyzer 400E	

Sample Invalid Log

An example of a log format that the system would be unable to preview and would fail validation.

In this case, the file cannot be properly parsed due to the fact that the json is malformed and lacks a closing brace.

File name	File content
InvalidLog.json	{"ip":"123.123.123.123", "uid":"507f1f77bcf86cd799439011"

Sample Valid Log File

FortinetLog.csv

src-ip	src-port	id	message	time	MAC-addr
23.59.154.35	58012	13002013	port-unreachable	1621824856	00:1A:C2:7B:00:47
23.59.154.35	58012	2100000014	health-check-timeout	1621824857	00:1A:C2:7B:00:49
23.59.154.35	58012	20033	ack	1621824858	00:1A:C2:7B:00:42
23.59.154.35	58012	5013	ack	1621824859	00:1A:C2:7B:00:46
23.59.154.35	58012	9990213	port-unreachable	1621824867	00:1A:C2:7B:00:41
23.59.154.35	58012	2.9E+10	port-unreachable	1621824877	00:1A:C2:7B:00:43
23.59.154.35	58012	127830013	port-unreachable	1621824887	00:1A:C2:7B:00:44