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})$

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"

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 Log File

FortiGate East-Aus 7121F

```
date=2019-05-10 time=11:37:47 logid="0000000013" type="traffic" subtype="forward" level="notice"
vd="vdom1" eventtime=1557513467369913239 srcip=10.1.100.11
srcport=58012 srcintf="port12" srcintfrole="undefined" dstip=23.59.154.35 dstport=80 dstintf="
port11" dstintfrole="undefined" srcuuid="ae28f494-5735-51e9-f247-d1d2ce663f4b"
dstuuid="ae28f494-5735-51e9-f247-d1d2ce663f4b" poluuid="ccb269e0-5735-51e9-a218-a397dd08b7eb"
sessionid=105048 proto=6 action="close" policyid=1 policytype="policy"
service="HTTP" dstcountry="Canada" srccountry="Reserved" trandisp="snat" transip=172.16.200.2
transport=58012 appid=34050 app="HTTP.BROWSER_Firefox" appcat="Web.Client"
apprisk="elevated" applist="g-default" duration=116 sentbyte=1188 rcvdbyte=1224 sentpkt=17
rcvdpkt=16 utmaction="allow" countapp=1 osname="Ubuntu" mastersrcmac="a2:e9:00:ec:40:01"
srcmac="a2:e9:00:ec:40:01" srcserver=0 utmref=65500-742
date=2019-05-10 time=11:37:48 logid="0000000014" type="traffic" subtype="forward" level="notice"
vd="vdom1" eventtime=1557513467369913239 srcip=10.1.100.11
srcport=58012 srcintf="port12" srcintfrole="undefined" dstip=23.59.154.35 dstport=80 dstintf="
port11" dstintfrole="undefined" srcuuid="ae28f494-5735-51e9-f247-d1d2ce663f4b"
dstuuid="ae28f494-5735-51e9-f247-d1d2ce663f4b" poluuid="ccb269e0-5735-51e9-a218-a397dd08b7eb"
sessionid=105048 proto=6 action="close" policyid=1 policytype="policy"
service="HTTP" dstcountry="Canada" srccountry="Reserved" trandisp="snat" transip=172.16.200.2
transport=58012 appid=34050 app="HTTP.BROWSER_Firefox" appcat="Web.Client"
apprisk="elevated" applist="g-default" duration=116 sentbyte=1188 rcvdbyte=1224 sentpkt=17
rcvdpkt=16 utmaction="allow" countapp=1 osname="Ubuntu" mastersrcmac="a2:e9:00:ec:40:01"
srcmac="a2:e9:00:ec:40:01" srcserver=0 utmref=65500-742
date=2019-05-10 time=11:37:49 logid="0000000015" type="traffic" subtype="forward" level="notice"
vd="vdom1" eventtime=1557513467369913239 srcip=10.1.100.11
srcport=58012 srcintf="port12" srcintfrole="undefined" dstip=23.59.154.35 dstport=80 dstintf="
port11" dstintfrole="undefined" srcuuid="ae28f494-5735-51e9-f247-d1d2ce663f4b"
dstuuid="ae28f494-5735-51e9-f247-d1d2ce663f4b" poluuid="ccb269e0-5735-51e9-a218-a397dd08b7eb"
sessionid=105048 proto=6 action="close" policyid=1 policytype="policy"
service="HTTP" dstcountry="Canada" srccountry="Reserved" trandisp="snat" transip=172.16.200.2
transport=58012 appid=34050 app="HTTP.BROWSER_Firefox" appcat="Web.Client"
apprisk="elevated" applist="g-default" duration=116 sentbyte=1188 rcvdbyte=1224 sentpkt=17
rcvdpkt=16 utmaction="allow" countapp=1 osname="Ubuntu" mastersrcmac="a2:e9:00:ec:40:01"
srcmac="a2:e9:00:ec:40:01" srcserver=0 utmref=65500-742
date=2019-05-10 time=11:37:50 logid="0000000016" type="traffic" subtype="forward" level="notice"
vd="vdom1" eventtime=1557513467369913239 srcip=10.1.100.11
srcport=58012 srcintf="port12" srcintfrole="undefined" dstip=23.59.154.35 dstport=80 dstintf="
port11" dstintfrole="undefined" srcuuid="ae28f494-5735-51e9-f247-d1d2ce663f4b"
dstuuid="ae28f494-5735-51e9-f247-d1d2ce663f4b" poluuid="ccb269e0-5735-51e9-a218-a397dd08b7eb"
sessionid=105048 proto=6 action="close" policyid=1 policytype="policy"
service="HTTP" dstcountry="Canada" srccountry="Reserved" trandisp="snat" transip=172.16.200.2
transport=58012 appid=34050 app="HTTP.BROWSER_Firefox" appcat="Web.Client"
apprisk="elevated" applist="g-default" duration=116 sentbyte=1188 rcvdbyte=1224 sentpkt=17
rcvdpkt=16 utmaction="allow" countapp=1 osname="Ubuntu" mastersrcmac="a2:e9:00:ec:40:01"
srcmac="a2:e9:00:ec:40:01" srcserver=0 utmref=65500-742
```