LOGStra

Input Formats | Output Formats | Normalisation Mappings | Types

Search

EDIT INPUT FORMAT

Fortinet Log v121

SAVE

SAMPLE LOGS

+ UPLOAD

Fortinet Log 14/02/2021

+ VALIDATE

+ PREVIEW

FIELD NAME		FIELD TYPE
src-ip	→	IPv4 (Suggested)
src-port	→	port (Suggested)
id	→	Device-Id (Suggested)
message	→	Message (Suggested)
time	→	Enter Type
Enter Name	→	Enter Type

CANCEL

SAVE

LOGStra

Input Formats | Output Formats | Normalisation Mappings | Types

Search

EDIT INPUT FORMAT

Fortinet Log v121

SAMPLE LOGS

+ UPLOAD

Fortinet Log 14/02/2021

+ VALIDATE

+ PREVIEW

FIELD NAME		FIELD TYPE
src-ip	→	IPv4 (Suggested)
src-port	→	port (Suggested)
id	→	Device-Id (Suggested)
message	→	Message (Suggested)
time	→	EPOCH
Enter Name	→	Enter Type

CANCEL

SAVE

LOGStra

Input Formats | Output Formats | Normalisation Mappings | Types

Search

EDIT INPUT FORMAT

Fortinet Log v121

SAMPLE LOGS

+ UPLOAD

Fortinet Log 14/02/2021

+ VALIDATE

+ PREVIEW

FIELD NAME		FIELD TYPE
src-ip	→	IPv4 (Suggested)
src-port	→	port (Suggested)
id	→	Device-Id (Suggested)
message	→	Message (Suggested)
time	→	EPOCH
MAC-addr	→	mac

CANCEL

SAVE

EDIT FORMAT

Enter Document Name

src-ip	→	IPv4
src-port	→	port
id	→	device-id
time	→	UTC
message	→	Message

+ SUBMIT

dir_11

Search

Favourites

Locations

Tags

Name	Size	Kind
Broken.json	558 bytes	JSON
FortinetLog.csv	558 bytes	Comm...et (.csv)
FortinetLog2.csv	558 bytes	Comm...et (.csv)
CatalystC3560Cx-8PC.csv	5 bytes	Comm...et (.csv)
FirePower4112.csv	5 bytes	Comm...et (.csv)
FortiAnalyzer400E.csv	5 bytes	Comm...et (.csv)
FortiGate-3980E.csv	5 bytes	Comm...et (.csv)
Nexus9500xGX.csv	5 bytes	Comm...et (.csv)

dir_11

Search

Favourites

Locations

Tags

Name	Size	Kind
Broken.json	558 bytes	JSON
FortinetLog.csv	558 bytes	Comm...et (.csv)
FortinetLog2.csv	558 bytes	Comm...et (.csv)
CatalystC3560Cx-8PC.csv	5 bytes	Comm...et (.csv)
FirePower4112.csv	5 bytes	Comm...et (.csv)
FortiAnalyzer400E.csv	5 bytes	Comm...et (.csv)
FortiGate-3980E.csv	5 bytes	Comm...et (.csv)
Nexus9500xGX.csv	5 bytes	Comm...et (.csv)

dir_11

Search

Favourites

Locations

Tags

Name	Size	Kind
Broken.json	558 bytes	JSON
FortinetLog.csv	558 bytes	Comm...et (.csv)
FortinetLog2.csv	558 bytes	Comm...et (.csv)
CatalystC3560Cx-8PC.csv	5 bytes	Comm...et (.csv)
FirePower4112.csv	5 bytes	Comm...et (.csv)
FortiAnalyzer400E.csv	5 bytes	Comm...et (.csv)
FortiGate-3980E.csv	5 bytes	Comm...et (.csv)
Nexus9500xGX.csv	5 bytes	Comm...et (.csv)

LOGStra

Input Formats | Output Formats | Normalisation Mappings | Types

Search

EDIT INPUT FORMAT

Fortinet Log v121

SAMPLE LOGS

+ UPLOAD

Fortinet Log 14/02/2021

+ VALIDATE

+ PREVIEW

FIELD NAME		FIELD TYPE
src-ip	→	IPv4 (Suggested)
src-port	→	port (Suggested)
id	→	Device-Id (Suggested)
message	→	Message (Suggested)
time	→	EPOCH
Enter Name	→	Enter Type

CANCEL

SAVE

LOGStra

Input Formats | Output Formats | Normalisation Mappings | Types

Search

EDIT INPUT FORMAT

Fortinet Log v121

SAMPLE LOGS

+ UPLOAD

Fortinet Log 14/02/2021

+ VALIDATE

+ PREVIEW

FIELD NAME		FIELD TYPE
src-ip	→	IPv4 (Suggested)
src-port	→	port (Suggested)
id	→	Device-Id (Suggested)
message	→	Message (Suggested)
time	→	EPOCH
MAC-addr	→	Enter Type

CANCEL

SAVE

Created new Input Format -

MS250-24P-South-Aus

Go Home

Save As: format.csv

Tags:

formats

Search

Favourites

Locations

Tags

Name	Date Modified	Size	Kind

Online Locations

File Format: Comma-separated Values (.csv)

Options...

New Folder

Cancel

Save

Suggested

device-id

All

IPv4

IPv6

Fortinet ID

MAC

Message

UTC

Suggested

port

All

IPv4

IPv6

Fortinet ID

MAC

Message

UTC

Suggested

IPv4

All

IPv6

Fortinet ID

MAC

Message

Port

UTC

Suggested

UTC

All

IPv4

IPv6

Fortinet ID

MAC

Message

Port

Suggested

All

IPv4

IPv6

Fortinet ID

MAC

Message

Port

CREATE INPUT FORMAT

SAVE

INPUT FORMAT NAME

Fortinet Log

UPLOADS

+ UPLOAD

Fortinet Log	14/05/2021

CANCEL

CREATE

CREATE INPUT FORMAT

Fortinet Log v121

SAVED

EDIT FORMAT

MS250-24P-South-Aus

src-ip	→	IPv4
src-port	→	port
id	→	device-id
time	→	UTC
message	→	Message

+ SUBMIT

LOGStra

Input Formats | Output Formats | Normalisation Mappings | Types

Search

INPUT FORMAT

+ CREATE

RECENT

MS250-24P-South-Aus	Now
Fortinet East-Aus #2md2	5 minutes ago
Fortinet East-Aus #2md2	5 minutes ago
Fortinet East-Aus #2md2	5 minutes ago

OUTPUT FORMAT

+ CREATE

RECENT

Fortinet East-Aus #2md2	5 minutes ago
Fortinet East-Aus #2md2	5 minutes ago
Fortinet East-Aus #2md2	5 minutes ago
Fortinet East-Aus #2md2	5 minutes ago

NORMALISATION MAPPINGS

+ CREATE

RECENT

Fortinet East-Aus #2md2	→	Splunk Cyber Security Team Alpha	5 minutes ago
Fortinet East-Aus #2md2	→	Splunk Cyber Security Team Alpha	5 minutes ago
Fortinet East-Aus #2md2	→	Splunk Cyber Security Team Alpha	5 minutes ago
Fortinet East-Aus #2md2	→	Splunk Cyber Security Team Alpha	5 minutes ago
Fortinet East-Aus #2md2	→	Splunk Cyber Security Team Alpha	5 minutes ago
Fortinet East-Aus #2md2	→	Splunk Cyber Security Team Alpha	5 minutes ago

CREATE INPUT FORMAT

INPUT FORMAT NAME

Name

UPLOADS

+ UPLOAD

CANCEL

CREATE

CREATE INPUT FORMAT

SAVE

INPUT FORMAT NAME

Fortinet Log v121

UPLOADS

+ UPLOAD

Fortinet Log	14/05/2021

CANCEL

CREATE

LOGStra

Input Formats | Output Formats | Normalisation Mappings | Types

Search

EDIT INPUT FORMAT

Fortinet Log v121

SAVE

SAMPLE LOGS

+ UPLOAD

FortinetLog 14/02/2021

+ VALIDATE + PREVIEW

Broken JSON Sample 05/03/2021

+ VALIDATE + PREVIEW

FIELD NAME		FIELD TYPE
src-ip	→	IPv4 (Suggested)
src-port	→	port (Suggested)
id	→	Device-Id (Suggested)
message	→	Message (Suggested)
time	→	EPOCH
MAC-addr	→	mac

CANCEL

SAVE

VALIDATION SUCCESS

THE SELECTED SAMPLE LOG WAS SUCCESSFULLY PARSED. LOG FORMAT WAS VALID, AND LOG CONTENTS MATCHED THE FORMAT FIELD TYPES.

CONTINUE

+ UPLOAD

CLONE

Fortinet East-Aus #2md2 → Splunk Cyber Security Team Alpha | 5 minutes ago ...

LOGStra

Input Formats | Output Formats | Normalisation Mappings | Types

Search

EDIT INPUT FORMAT

Fortinet Log v121

SAVE

SAMPLE LOGS

+ UPLOAD

FortinetLog 14/02/2021

+ VALIDATE + PREVIEW

Broken JSON Sample 05/03/2021

+ VALIDATE + PREVIEW

FortinetLog2 05/03/2021

+ VALIDATE + PREVIEW

FIELD NAME		FIELD TYPE
src-ip	→	IPv4 (Suggested)
src-port	→	port (Suggested)
id	→	Device-Id (Suggested)
message	→	Message (Suggested)
time	→	EPOCH
MAC-addr	→	mac

CANCEL

SAVE

VALIDATION FAILURE

FILE VALIDATION FAILED WITH THE FOLLOWING WARNING: THE SELECTED FILE CONTAINED INVALID JSON AND COULD NOT BE PARSED. PLEASE CHECK THAT YOU HAVE SELECTED THE CORRECT FILE.

CONTINUE

Edit

Delete

Save local copy

Create Mapping

NORMALISATION MAPPINGS

Search

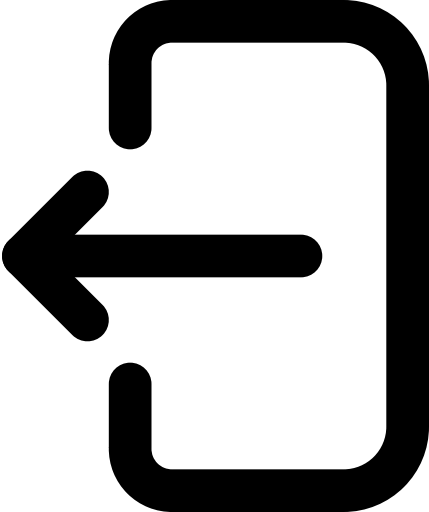
+ CREATE

Fortinet East-Aus #2md2	→	Splunk Cyber Security Team Alpha
Firepower 1150	→	Splunk Cyber Security Team Alpha
Firepower 1140	→	Splunk Cyber Security Team Alpha
Firepower 4145	→	Splunk Cyber Security Team Alpha
Catalyst C3560CX-12PC	→	Splunk Cyber Security Team Alpha
Catalyst C3560CX-8PC	→	Elastic Security Team - Dolan
Catalyst 9500 100/40-G	→	Elastic Security Team - Dolan
MS210-24	→	Elastic Security Team - Dolan
MS250-24P	→	Elastic Security Team - Dolan
Nexus 9500 X9716-GX	→	Elastic Security Team - Dolan

PREVIEW FAILURE

FILE PREVIEW FAILED WITH THE FOLLOWING WARNING: THE SELECTED FILE CONTAINED INVALID JSON AND COULD NOT BE PARSED. PLEASE CHECK THAT YOU HAVE SELECTED THE CORRECT FILE.

CONTINUE



Edit

Delete

Save local copy

Create Mapping

EDIT TYPES

TYPE		REGEX
IPv4	→	^(?:[0-9]{1,3}\.){3}[0-9]{1,3}$
IPv6	→	(([0-9a-fA-F]{1,4}:){7,7}[0-9a-fA-F]{1,4
Fortinet ID	→	\d{7,}
MAC	→	^([0-9A-Fa-f]{2}[:-]){5}([0-9A-Fa-f]{2})$
Message	→	*
UTC	→	\d{4}-(?:0[1-9]|1[0-2])-(?:0[1-9]|[1-2]\d
EPOCH	→	\d{10,}
	→	

SAVE

EDIT TYPES

TYPE		REGEX
IPv4	→	^(?:[0-9]{1,3}\.){3}[0-9]{1,3}$
IPv6	→	(([0-9a-fA-F]{1,4}:){7,7}[0-9a-fA-F]{1,4
Fortinet ID	→	\d{7,}
MAC	→	^([0-9A-Fa-f]{2}[:-]){5}([0-9A-Fa-f]{2})$
Message	→	*
UTC	→	\d{4}-(?:0[1-9]|1[0-2])-(?:0[1-9]|[1-2]\d
EPOCH	→	
	→	

SAVE

EDIT TYPES

TYPE		REGEX
IPv4	→	^(?:[0-9]{1,3}\.){3}[0-9]{1,3}$
IPv6	→	(([0-9a-fA-F]{1,4}:){7,7}[0-9a-fA-F]{1,4
Fortinet ID	→	\d{7,}
MAC	→	^([0-9A-Fa-f]{2}[:-]){5}([0-9A-Fa-f]{2})$
Message	→	*
UTC	→	\d{4}-(?:0[1-9]|1[0-2])-(?:0[1-9]|[1-2]\d
	→	

SAVE

HOME

INPUT FORMAT

+ CREATE

RECENT

Fortinet East-Aus #2md2	5 minutes ago
Firepower 4112	5 minutes ago
Catalyst C3560CX-8PC	5 minutes ago
MS250-24P	5 minutes ago

OUTPUT FORMAT

+ CREATE

RECENT

Splunk Cyber Security Team	5 days ago
Elastic Security Team	20 days ago

NORMALISATION MAPPINGS

+ CREATE

RECENT

Firepower 4112	→	Splunk Cyber Security Team Alpha	5 minutes ago
Fortinet East-Aus #2md2	→	Splunk Cyber Security Team Alpha	30 minutes ago
Catalyst C3560CX-8PC	→	Splunk Cyber Security Team Alpha	4 hours ago
MS250-24P	→	Elastic Security Team - Dolan	1 day ago
Firepower 1150	→	Splunk Cyber Security Team Alpha	3 days ago
Firepower 1150	→	Splunk Cyber Security Team Alpha	5 days ago

INPUT FORMATS

Search

+ CREATE

- Fortinet East-Aus #2md2
- Firepower 1150
- Firepower 4112
- Firepower 4145
- Catalyst C3560CX-12PC
- Catlayst C3560CX-8PC
- Catalyst 9500 100/40-G
- MS210-24
- MS210-24P
- MS250-24
- MS250-23P
- Nexus 9332D-GX2B
- Nexus 9332D-GX3B
- Nexus 9500 X9716-GX

OUTPUT FORMATS

Search

+ CREATE

Splunk Cyber Security Team Alpha •••

Elastic Security Team - Dolan •••

LOGStra

Input Formats | Output Formats | Normalisation Mappings | Types

Search

EDIT INPUT FORMAT

Fortinet Log v121

SAMPLE LOGS

+ UPLOAD

FortinetLog 14/02/2021

+ VALIDATE + PREVIEW

Broken JSON Sample 05/03/2021

+ VALIDATE + PREVIEW

FortinetLog2 05/03/2021

+ VALIDATE + PREVIEW

FIELD NAME		FIELD TYPE	PREVIEW
src-ip	→	IPv4 (Suggested)	10.1.100.11
src-port	→	port (Suggested)	58012
id	→	Device-Id (Suggested)	13002013
message	→	Message (Suggested)	PORT-UNREACHABLE
time	→	EPOCH	1621824857
MAC-addr	→	mac	00:1A:C2:7B:00:47

CANCEL

SAVE

CLOSE PREVIEW

VALIDATION FAILURE

FORMAT VALIDATION FAILED WITH THE FOLLOWING ERRORS:

FIELD ‘TIME’ DID NOT CONFORM TO THE SCHEMA FOR ‘EPOCH’

FIELD ‘ID’ DID NOT CONFORM TO THE SCHEMA FOR ‘DEVICE-ID’

CONTINUE

Edit

Delete

DELETE FORMAT

CONFIRM DELETE

ARE YOU SURE YOU WANT TO DELETE THE FORMAT FORTINET EAST-AUS #2MD2? DELETED FORMATS CANNOT BE RECOVERED.

DELETE CANCEL

CREATE MAPPING

SELECT INPUT FORMAT

Search

Fortinet East-Aus #2md2 + SELECT

Firepower 4112 + SELECT

Catalyst C3560CX-8PC + SELECT

MS250-24P + SELECT

SELECT OUTPUT FORMAT

Search

Splunk Cyber Security Team Alpha + SELECT

Splunk V1 + SELECT

Splunk V3 + SELECT

Elastic Security Team + SELECT

CREATE MAPPING

FORTINET LOG V121 → SPLUNK V3

INPUT FIELDS	→	OUTPUT FIELDS
	→	Source_Destination
srcport (Suggested)	→	Source_Port
	→	Network_Log
	→	Type_Class
logid (Suggested)	→	id
time (Suggested)	→	eventTime

Save

HOME

INPUT FORMAT

+ CREATE

RECENT

Fortilog v121	1 minutes ago
Fortinet East-Aus #2md2	5 minutes ago
Firepower 4112	5 minutes ago
Catalyst C3560CX-8PC	5 minutes ago
MS250-24P	5 minutes ago

OUTPUT FORMAT

+ CREATE

RECENT

Splunk Cyber Security Team	5 days ago
Elastic Security Team	20 days ago

NORMALISATION MAPPINGS

+ CREATE

RECENT

Fortilog v121	→	Splunk V3	now
Fortinet East-Aus #2md2	→	Splunk Cyber Security Team Alpha	30 minutes ago
Catalyst C3560CX-8PC	→	Splunk Cyber Security Team Alpha	4 hours ago
MS250-24P	→	Elastic Security Team - Dolan	1 day ago
Firepower 1150	→	Splunk Cyber Security Team Alpha	3 days ago
Firepower 1150	→	Splunk Cyber Security Team Alpha	5 days ago

CREATE MAPPING

SELECT INPUT FORMAT

Fortinet log

SELECT OUTPUT FORMAT

Search

Fortinet Log v121 — SELECT

Splunk Cyber Security Team Alpha — SELECT

Splunk V1 — SELECT

Splunk V3 — SELECT

Elastic Security Team — SELECT

CREATE MAPPING

FORTINET LOG V121 → SPLUNK V3

INPUT FIELDS		OUTPUT FIELDS
src_ip	→	Source_Destination
srcport (Suggested)	→	Source_Port
	→	Network_Log
	→	Type_Class
logid (Suggested)	→	id
time (Suggested)	→	eventTime

Save

CREATE MAPPING FORTINET LOG V121 →

SELECT INPUT FORMAT

Fortinet log

Fortinet Log v121 — SELECTED

SELECT OUTPUT FORMAT

Search

- Splunk Cyber Security Team Alpha — + SELECT
- Splunk V1 — + SELECT
- Splunk V3 — + SELECT
- Elastic Security Team — + SELECT

CREATE MAPPING

FORTINET LOG V121 → SPLUNK V3

INPUT FIELDS	→	OUTPUT FIELDS
src_ip	→	Source_Destination
srcport (Suggested)	→	Source_Port
level	→	Network_Log
	→	Type_Class
logid (Suggested)	→	id
time (Suggested)	→	eventTime

Save

Suggestions

subtype 1

srcname

All

dst ip

level

time

srcname

srcport

logid

subtype 1

CREATE MAPPING

FORTINET LOG V121 JAVA

SELECT INPUT FORMAT

Fortinet log

Fortinet Log v121 Java — SELECTED

SELECT OUTPUT FORMAT

Splunk

Splunk Cyber Security Team Alpha — SELECT

Splunk V2 — SELECT

Splunk V3 — SELECT

CREATE MAPPING

FORTINET LOG V121 → **SPLUNK V3**

INPUT FIELDS		OUTPUT FIELDS
src_ip	→	Source_Destination
srcport (Suggested)	→	Source_Port
level	→	Network_Log
subtype 1	→	Type_Class
logid (Suggested)	→	id
time (Suggested)	→	eventTime

Save

NORMALISATION MAPPING

FORTINET LOG V121 → SPLUNK V3

SAVE

INPUT FIELDS		OUTPUT FIELDS
srcip	→	Source_Destination
srcport	→	Source_Port
level	→	Network_Log
subtype	→	Type_Class
logid	→	id
time	→	eventTime

CREATE MAPPING FORTINET LOG V121 → SPLUNK V3

SELECT INPUT FORMAT

Fortinet log

SELECT OUTPUT FORMAT

Splunk

Fortinet Log v121 Java SELECTED

Splunk V3 SELECTED

Continue

NORMALISATION MAPPING

FORTINET LOG V121 → SPLUNK V3

SAVE

INPUT FIELDS		OUTPUT FIELDS
dstip	→	Source_Destination
srcport	→	Source_Port
level	→	Network_Log
subtype	→	Type_Class
logid	→	id
time	→	eventTime