EDIT INPUT FORMAT

FortiGate East-Aus 7121F

SAMPLE LOGS

+ UPLOAD

FortiGate Sample 4f3 14/02/2021

+ VALIDATE + PREVIEW

FortiGate Sample F83 05/03/2021

+ VALIDATE + PREVIEW

Broken JSON Sample 05/03/2021

+ VALIDATE + PREVIEW

FIELD NAME		FIELD TYPE
src-ip	→	IPv4
src-port	→	port
id	→	Device-Id
time	→	UTC
message	→	Message
MAC-addr	→	mac

CANCEL

SAVE

EDIT FORMAT

Enter Document Name

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

+ SUBMIT

EDIT INPUT FORMAT

FortiGate East-Aus 7121F

SAMPLE LOGS

+ UPLOAD

FortiGate Sample 4f3 14/02/2021

+ VALIDATE + PREVIEW

FortiGate Sample F83 05/03/2021

+ VALIDATE + PREVIEW

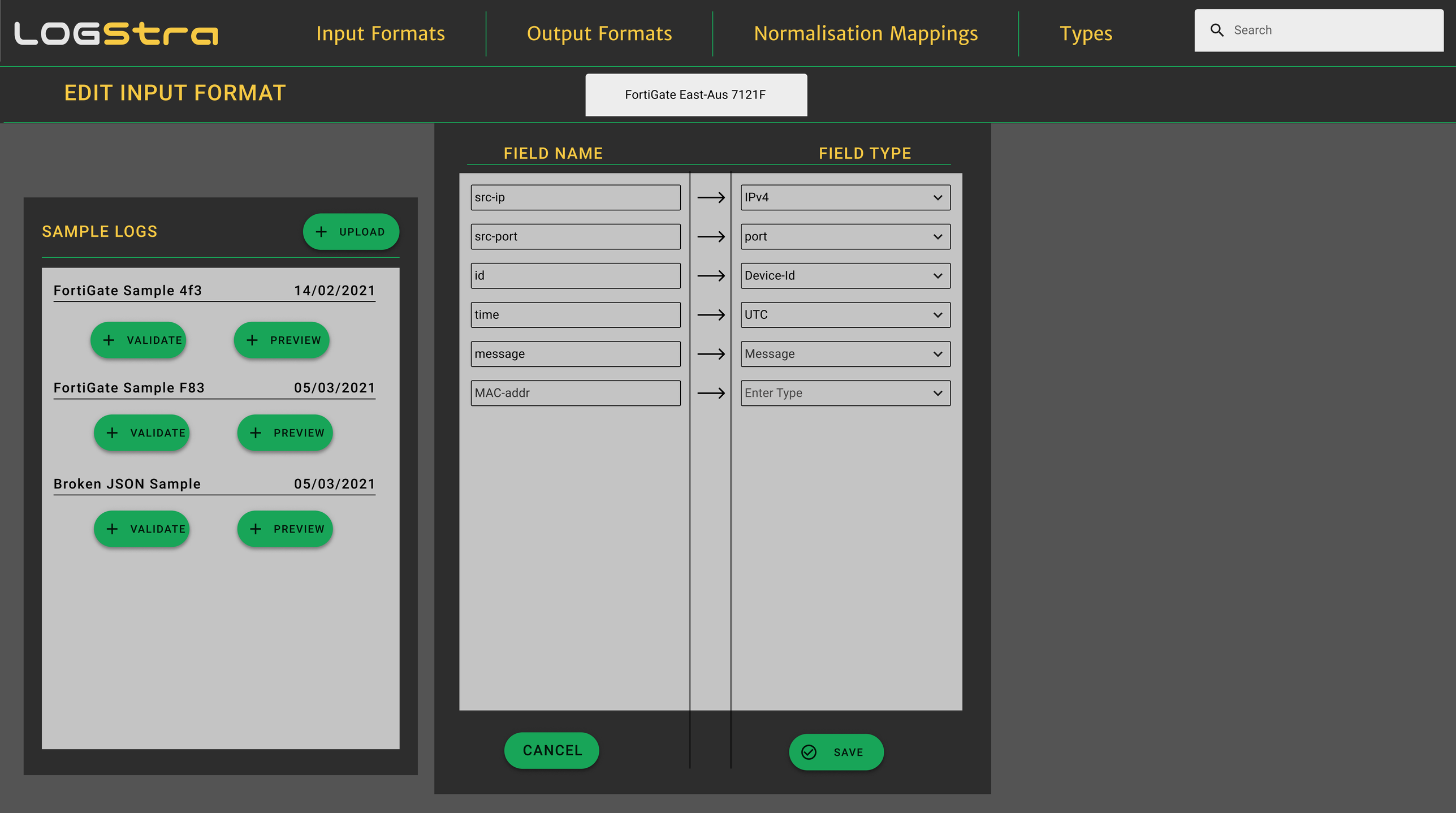
Broken JSON Sample 05/03/2021

+ VALIDATE + PREVIEW

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

CANCEL

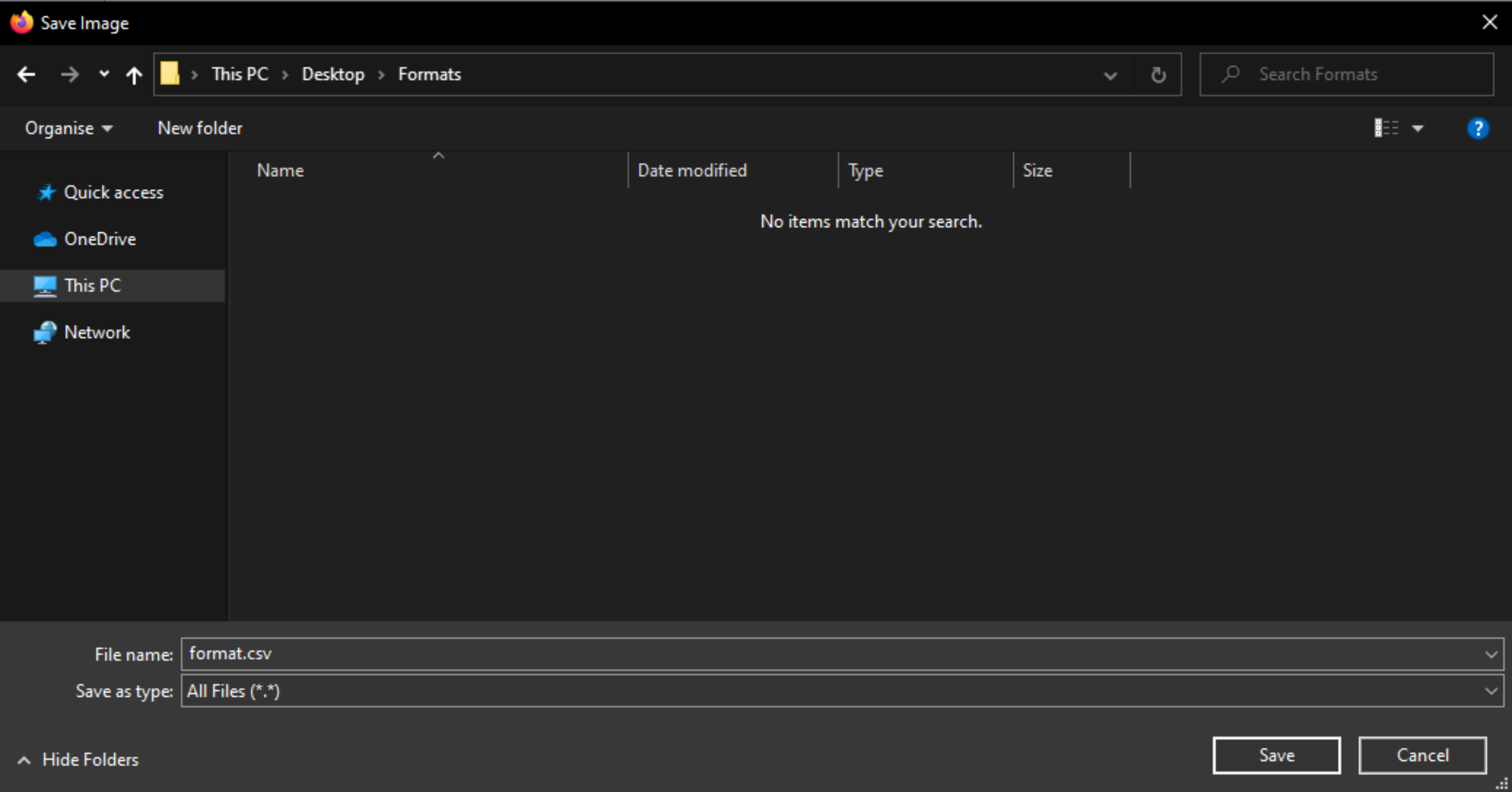
SAVE

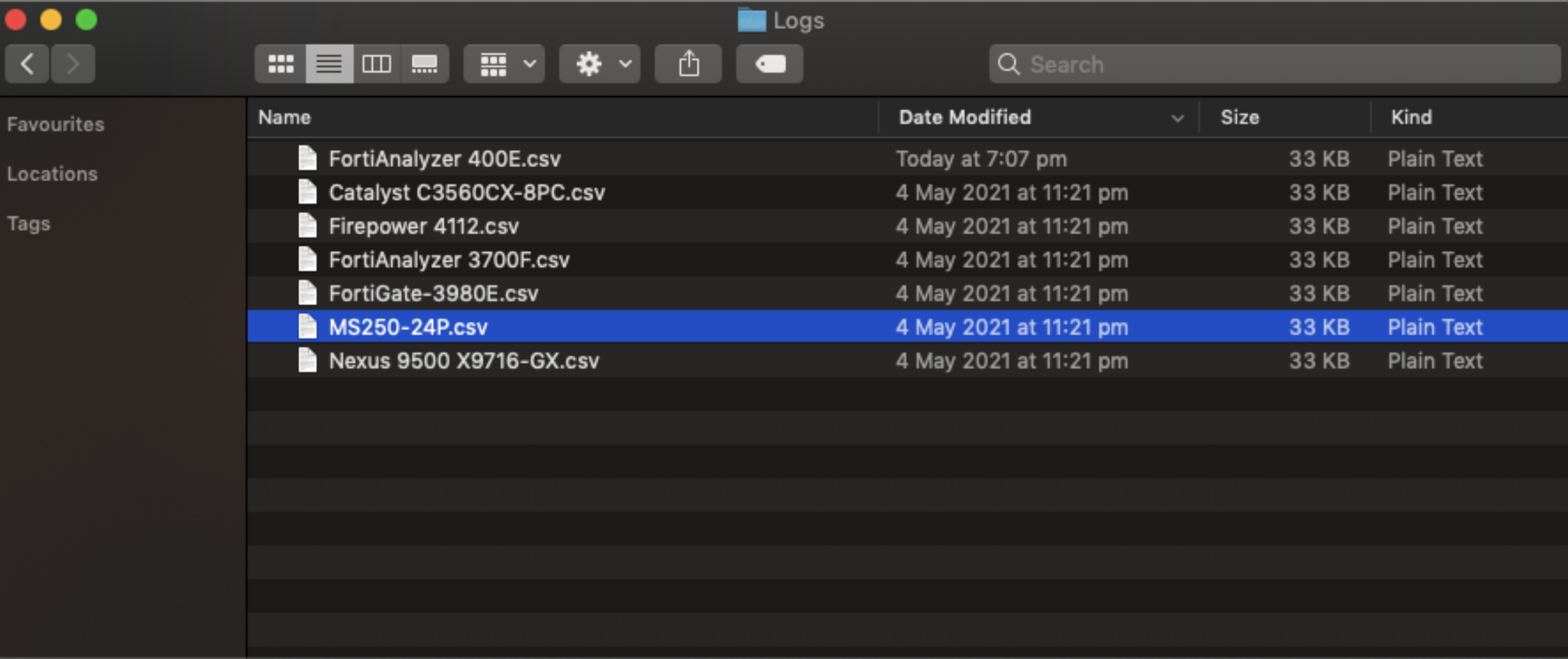

LOGStra
Input Formats
Output Formats
Normalisation Mappings
Types
Search
EDIT INPUT FORMAT
FortiGate East-Aus 7121F
SAMPLE LOGS
+ UPLOAD
FortiGate Sample 4f3
14/02/2021
+ VALIDATE
+ PREVIEW
FortiGate Sample F83
05/03/2021
+ VALIDATE
+ PREVIEW
Broken JSON Sample
05/03/2021
+ VALIDATE
+ PREVIEW
FIELD NAME
FIELD TYPE
src-ip
IPv4
src-port
port
id
Device-Id
time
UTC
message
Message
MAC-addr
Enter Type
CANCEL
SAVE

Created new Input Format -

MS250-24P-South-Aus

Go Home


Save Image
This PC
Desktop
Formats
Search Formats
Organise
New folder
Name
Date modified
Type
Size
Quick access
OneDrive
This PC
Network
No items match your search.
File name:
format.csv
Save as type:
All Files (*.*)
Hide Folders
Save
Cancel


Logs
Search
Favourites
Locations
Tags
Name
Date Modified
Size
Kind
FortiAnalyzer 400E.csv
Today at 7:07 pm
33 KB
Plain Text
Catalyst C3560CX-8PC.csv
4 May 2021 at 11:21 pm
33 KB
Plain Text
Firepower 4112.csv
4 May 2021 at 11:21 pm
33 KB
Plain Text
FortiAnalyzer 3700F.csv
4 May 2021 at 11:21 pm
33 KB
Plain Text
FortiGate-3980E.csv
4 May 2021 at 11:21 pm
33 KB
Plain Text
MS250-24P.csv
4 May 2021 at 11:21 pm
33 KB
Plain Text
Nexus 9500 X9716-GX.csv
4 May 2021 at 11:21 pm
33 KB
Plain Text

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

INPUT FORMAT NAME

FortiGate East

SAMPLE LOGS

+ ADDED

MS250-24P	14/02/2021

CANCEL

CREATE

CREATE INPUT FORMAT

FortiGate East-Aus 7121F

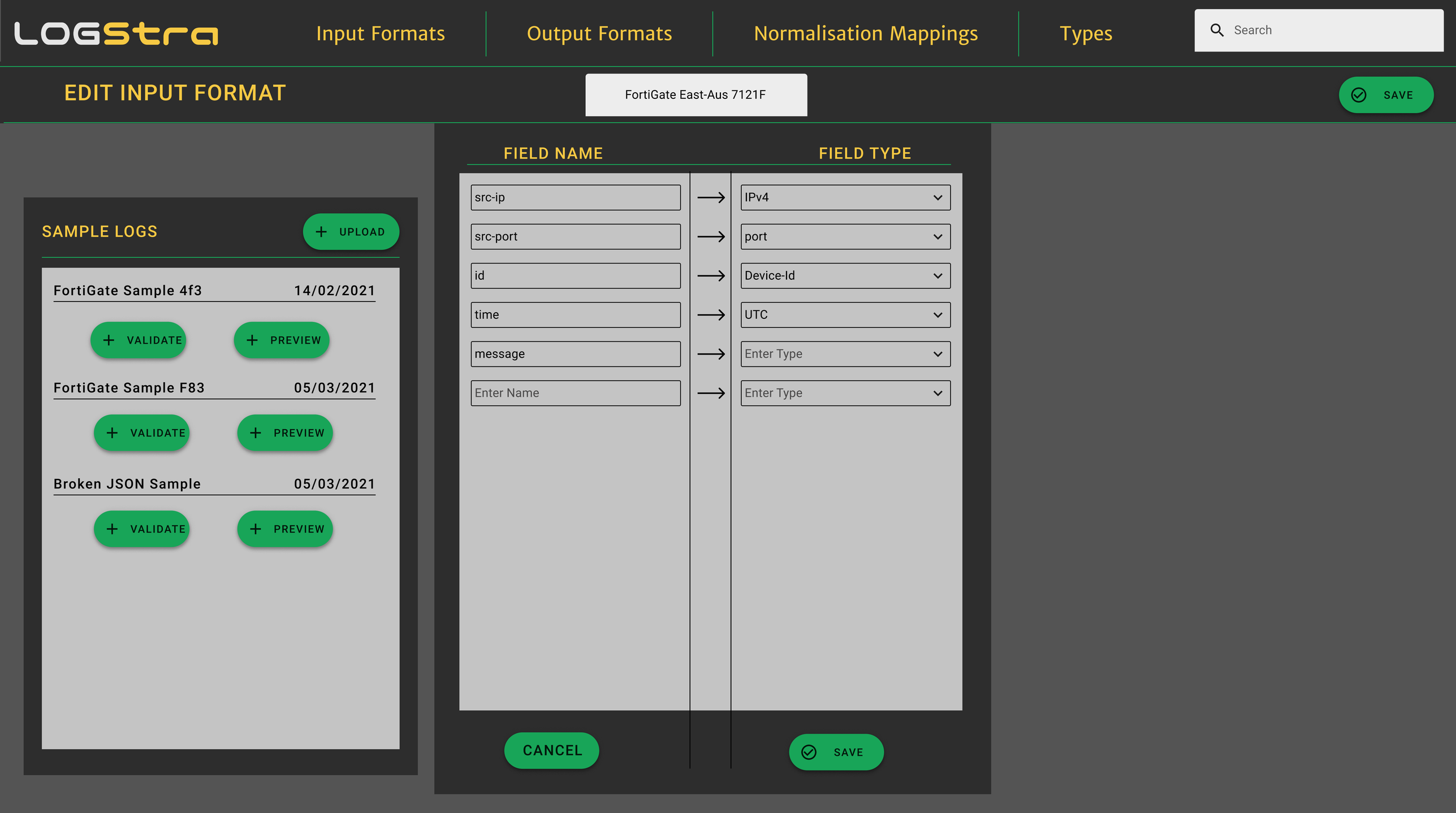
SAVED

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
EDIT INPUT FORMAT
FortiGate East-Aus 7121F
SAVE
SAMPLE LOGS
UPLOAD
FortiGate Sample 4f3
14/02/2021
VALIDATE
PREVIEW
FortiGate Sample F83
05/03/2021
VALIDATE
PREVIEW
Broken JSON Sample
05/03/2021
VALIDATE
PREVIEW
FIELD NAME
FIELD TYPE
src-ip
IPv4
src-port
port
id
Device-Id
time
UTC
message
Enter Type
Enter Name
Enter Type
CANCEL
SAVE

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

SAMPLE LOGS

+ UPLOAD

CANCEL

CREATE

CREATE INPUT FORMAT

SAVE

INPUT FORMAT NAME

FortiGate East-Aus 7121F

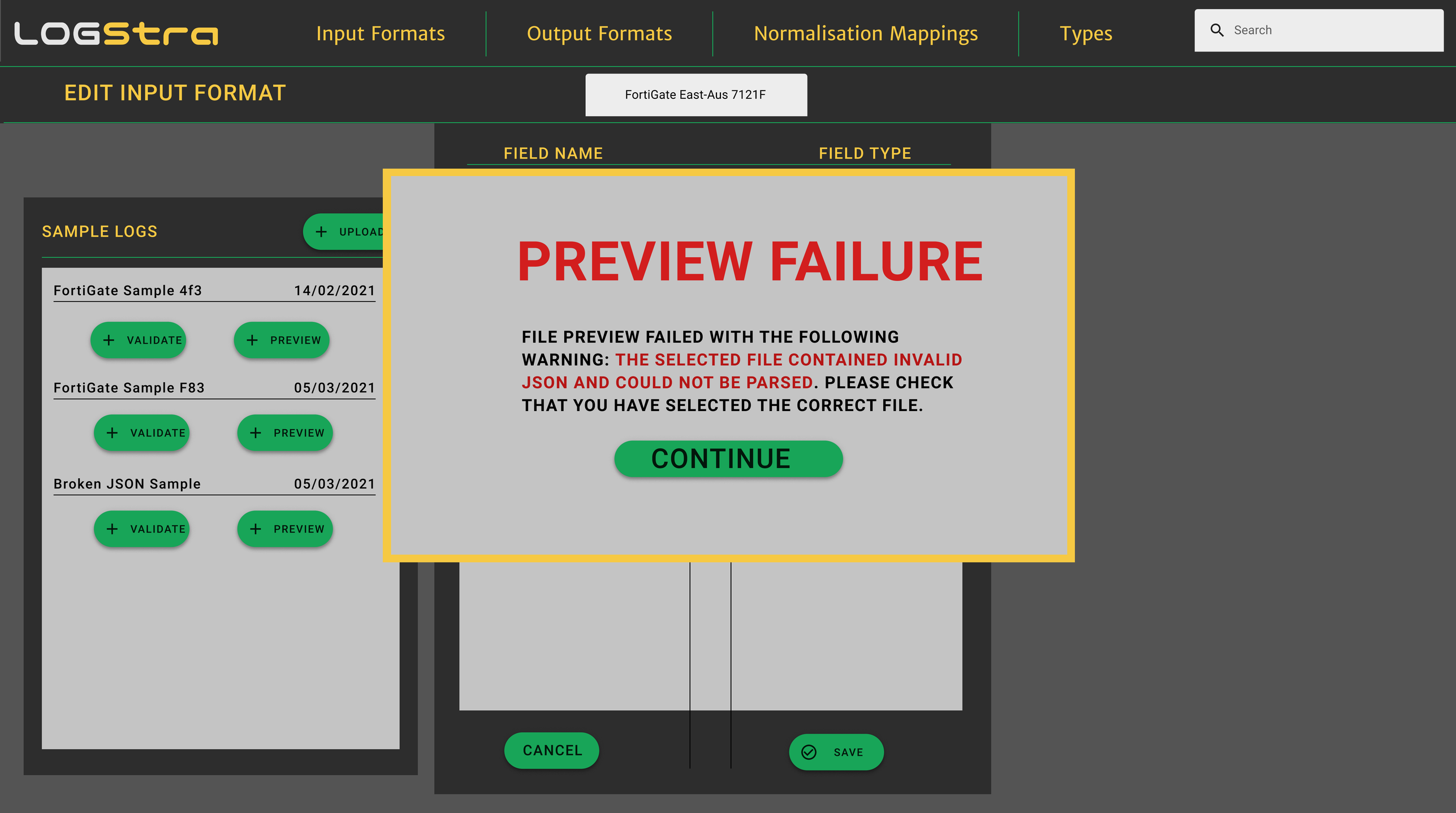
SAMPLE LOGS

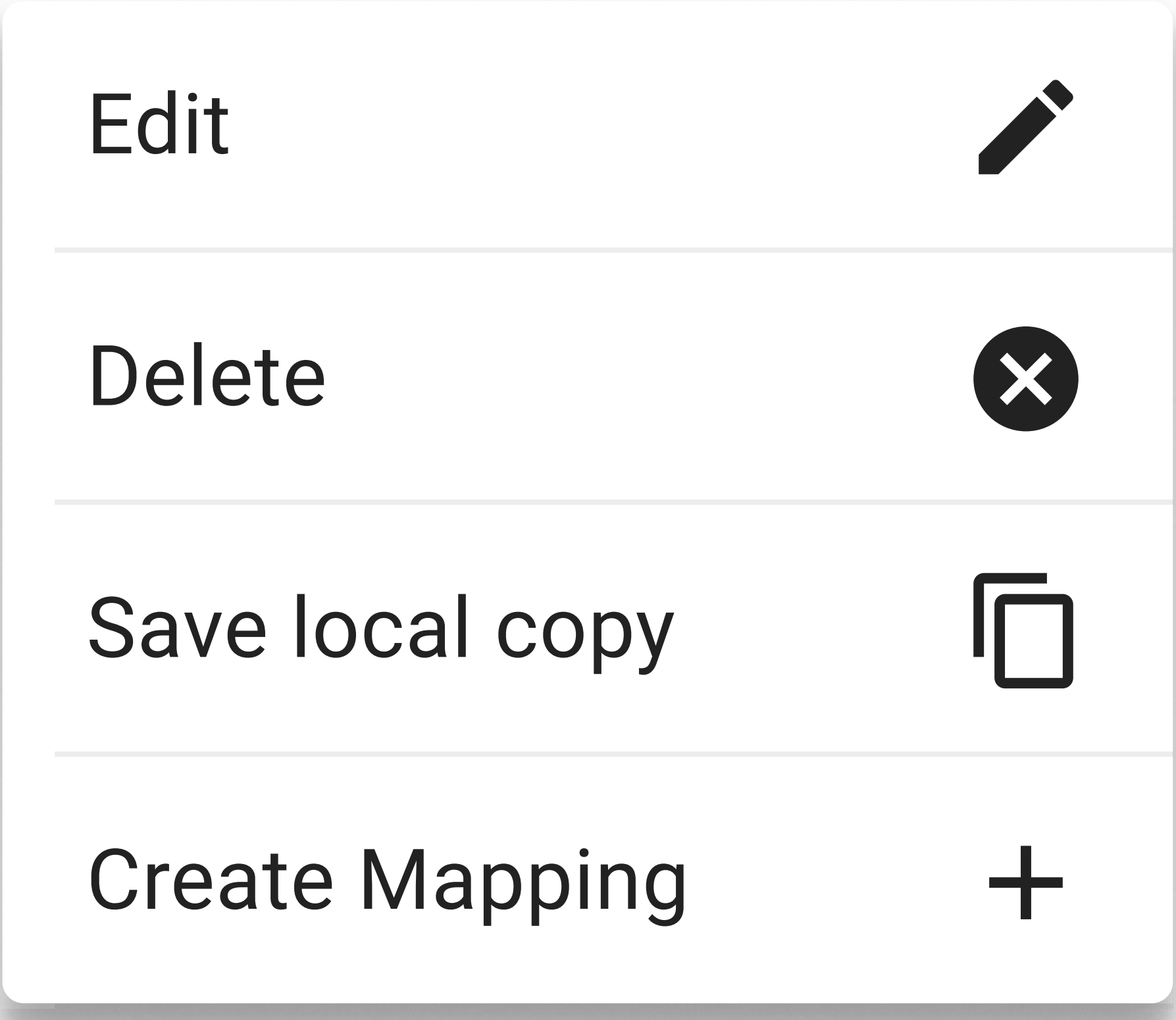
+ ADDED

CANCEL

CREATE


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


LOGStra
Input Formats
Output Formats
Normalisation Mappings
Types
Search
EDIT INPUT FORMAT
FortiGate East-Aus 7121F
FIELD NAME
FIELD TYPE
SAMPLE LOGS
+ UPLOAD
FortiGate Sample 4f3
14/02/2021
+ VALIDATE
+ PREVIEW
FortiGate Sample F83
05/03/2021
+ VALIDATE
+ PREVIEW
Broken JSON Sample
05/03/2021
+ VALIDATE
+ PREVIEW
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
CANCEL
SAVE


Edit
Delete
Save local copy
Create Mapping