

Decoders Syntax

Options

- [decoder](#)
- [parent](#)
- [accumulate](#)
- [program_name](#)
- [prematch](#)
- [regex](#)
- [order](#)
- [fts](#)
- [ftscomment](#)

decoder

The attributes list below defines a decoder.

Default Value	n/a
Allowed values	n/a

The attributes list below defines a decoder.

Attribute	Description
id	The ID of the decoder
name	The name of the decoder
type	The type of the decoder
status	The status of the decoder


parent

It is used to link a subordinate codeblock to his parent.

Default Value	n/a
Allowed values	Any decoder name

accumulate

Allow OSSEC to track events over multiple log messages based on a decoded id.

 **Note**

Requires a regex populating the id field.

Default Value	n/a
Allowed values	n/a

program_name

It defines the name of the program with which the decoder is associated.

Default Value	n/a
Allowed values	Any sregex expression

prematch

It attempts to find a match within the log for the string defined.

Default Value	n/a
Allowed values	Any sregex expression

regex

Default Value	n/a
Allowed values	Any regex expression

order

It defines what the parenthesis groups contain and the order in which they were received.

Default Value	n/a	
Static fields	srcuser	Extracts the source username
	dstuser	Extracts the destination (target) username
	user	An alias to dstuser (only one of the two can be used)
	srcip	Source ip
	dstip	Destination ip
	srcport	Source port
	dstport	Destination port
	protocol	Protocol
	id	Event id
	url	Url of the event
	action	Event action (deny, drop, accept, etc)
	status	Event status (success, failure, etc)
	extra_data	Any extra data
Dynamic fields	Any string not included in the previous list	

fts

It is used to designate a decoder as one in which the first time it matches the administrator would like to be alerted.

Default Value	n/a	
Allowed values	location	Where the log came from
	srcuser	Extracts the source username
	dstuser	Extracts the destination (target) username
	user	An alias to dstuser (only one of the two can be used)
	srcip	Source ip
	dstip	Destination ip
	srcport	Source port

dstport	Destination port
protocol	Protocol
id	Event id
url	Url of the event
action	Event action (deny, drop, accept, etc)
status	Event status (success, failure, etc)
extra_data	Any extra data

ftscomment

It adds a comment to a decoder when *<fts>* tag is used.

Default Value	n/a
Allowed values	Any string