

Rules Syntax

Available options

- [rule](#)
- [match](#)
- [regex](#)
- [decoded_as](#)
- [category](#)
- [field](#)
- [srcip](#)
- [dstip](#)
- [extra_data](#)
- [user](#)
- [program_name](#)
- [hostname](#)
- [time](#)
- [weekday](#)
- [id](#)
- [url](#)
- [if_sid](#)
- [if_group](#)
- [if_level](#)
- [if_matched_sid](#)
- [if_matched_group](#)
- [same_id](#)
- [same_source_ip](#)
- [same_source_port](#)
- [same_dst_port](#)
- [same_location](#)
- [same_user](#)
- [description](#)
- [list](#)
- [info](#)
- [options](#)
- [check_diff](#)
- [group](#)

rule

level	Definition	Specifies the level of the rule. Alerts and responses use this value.
	Allowed values	0 to 16
id	Definition	Specifies the ID of the rule.
	Allowed values	Any number from 1 to 9999
maxsize	Definition	Specifies the maximum size of the event.

	Allowed values	from 1 to 99999
frequency	Definition	Number of times the rule must have matched before firing. Triggers when 2 more than this setting.
	Allowed values	Any number from 1 to 9999
timeframe	Definition	The timeframe in seconds. This option is intended to be used with the frequency option.
	Allowed values	Any number from 1 to 9999
ignore	Definition	The time (in seconds) to ignore this rule after firing it (to avoid floods).
	Allowed values	Any number from 1 to 9999
overwrite	Definition	Used to supercede an OSSEC rule with local changes.
	Allowed values	yes

match

Any string to match against the log event.

Default Value	n/a
Allowed values	Any sregex expression

regex

Any regex to match against the log event.

Default Value	n/a
Allowed values	Any regex expression

decoded_as

Default Value	n/a
Allowed values	Any decoder name

category

The decoded category to match: ids, syslog, firewall, web-log, squid or windows.

Default Value	n/a
Allowed values	Any category

field

Any regex to be compared to a field extracted by the decoder.

name	Specifies the name of the field extracted by the decoder.
------	---

srcip

Any IP address or CIDR block to be compared to an IP decoded as srcip. Use “!” to negate it.

Default Value	n/a
Allowed values	Any srcip

dstip

Any IP address or CIDR block to be compared to an IP decoded as dstip. Use “!” to negate it.

Default Value	n/a
Allowed values	Any dstip

extra_data

Any string that is decoded into the extra_data field.

Default Value	n/a
Allowed values	Any string.

user

Any username (decoded as the username).

Default Value	n/a
Allowed values	Any sregex expression

program_name

Program name is decoded from syslog process name.

Default Value	n/a
Allowed values	Any sregex expression

hostname

Any hostname (decoded as the syslog hostname) or log file.

Default Value	n/a
Allowed values	Any sregex expression

time

Time that the event was generated.

Default Value	n/a
Allowed values	Any time range (hh:mm-hh:mm)

weekday

Week day that the event was generated.

Default Value	n/a
Allowed values	monday - sunday, weekdays, weekends

id

Any ID (decoded as the ID).

Default Value	n/a
Allowed values	Any sregex expression

url

Any URL (decoded as the URL).

Default Value	n/a
Allowed values	Any sregex expression

if_sid

Matches if the ID has matched.

Default Value	n/a
Allowed values	Any rule id

if_group

Matches if the group has matched before.

Default Value	n/a
Allowed values	Any Group

if_level

Matches if the level has matched before.


Default Value	n/a
Allowed values	Any level from 1 to 16

if_matched_sid

Matches if an alert of the defined ID has been triggered in a set number of seconds.

This option is used in conjunction with frequency and timeframe.

Default Value	n/a
Allowed values	Any rule id

 **Note**

Rules at level 0 are discarded immediately and will not be used with the if_matched_rules. The level must be at least 1, but the <no_log> option can be added to the rule to make sure it does not get logged.

if_matched_group

Matches if an alert of the defined group has been triggered in a set number of seconds.

This option is used in conjunction with frequency and timeframe.

Default Value	n/a
Allowed values	Any Group

same_id

Specifies that the decoded id must be the same. This option is used in conjunction with frequency and timeframe.

Default Value	n/a
Allowed values	n/a

same_source_ip

Specifies that the decoded source ip must be the same. This option is used in conjunction with frequency and timeframe.

Default Value	n/a
Allowed values	n/a

same_source_port

Specifies that the decoded source port must be the same. This option is used in conjunction with frequency and timeframe.

Default Value	n/a
Allowed values	n/a

same_dst_port

Specifies that the decoded destination port must be the same. This option is used in conjunction with frequency and timeframe.

Default Value	n/a
Allowed values	n/a

same_location

Specifies that the location must be the same. This option is used in conjunction with frequency and timeframe.

Default Value	n/a
Allowed values	n/a

same_user

Specifies that the decoded user must be the same. This option is used in conjunction with frequency and timeframe.

Default Value	n/a
Allowed values	n/a

description

Rule description.

Default Value	n/a
Allowed values	Any string

list

Preform a CDB lookup using an ossec list. This is a fast on disk database which will always find keys within two seeks of the file.

Default Value	n/a	
Allowed values	Path to the CDB file to be used for lookup from the OSSEC directory.Must also be included in the ossec.conf file.	

Attribute	Description	
field	key in the CDB: srcip, srcport, dstip, dstport, extra_data, user, url, id, hostname, program_name, status, action, dynamic field.	
lookup	match_key	key to search within the cdb and will match if they key is present. Default.
	not_match_key	key to search and will match if it is not present in the database.

	match_key_value	searched for in the cdb. It will be compared with regex from attribute check_value.
	address_match_key	IP and the key to search within the cdb and will match if they key is present.
	not_address_match_key	IP the key to search and will match if it IS NOT present in the database
	address_match_key_value	IP to search in the cdb. It will be compared with regex from attribute check_value.
check_value	regex for matching on the value pulled out of the cdb when using types: address_match_key_value, match_key_value	

info

Extra information may be added through the following attributes:

Default Value	n/a
Allowed values	Any string

Attribute	Allowed values	Description
type	text	This is the default when no type is selected. Additional,information about the alert/event.
	link	Link to more information about the alert/event.
	cve	The CVE Number related to this alert/event.
	ovsdb	The osvdb id related to this alert/event.

options

Additional rule options

Attribute	Description
alert_by_email	Always alert by email.
no_email_alert	Never alert by email.
no_log	Do not log this alert.

check_diff

Used to determine when the output of a command changes.

Default Value	n/a
Allowed values	n/a

group

Add additional groups to the alert. Groups are optional tags added to alerts.

They can be used by other rules by using if_group or if_matched_group, or by alert parsing tools to categorize alerts.

Default Value	n/a
Allowed values	Any String