Documentation › User manual › Reference › Local configuration › global

global

XML section name

```
<global>
</global>
```

Global configuration generally applies to features that affect the system as a whole, rather than just one component.

Options

- alerts_log
- email_notification
- email_to
- email_from
- email_reply_to
- smtp_server
- email_maxperhour
- email_idsname
- custom_alert_output
- stats
- logall
- memory_size
- white_list
- host_information
- jsonout_output
- prelude_output
- picviz_output
- picviz_socket
- zeromq_output
- zeromq_uri
- geoip_db_path

alerts_log

This enable or disable writing alerts to `/var/ossec/logs/alerts/alerts.log`.

Default value	yes
Allowed values	yes, no

⚠ Warning

Disabling JSON and plain text formated alerts simultaneously is not compatible with the integrator, syslog client and email features.

email_notification

This enable or disables email alerting.

Default value	no
Allowed values	yes, no

email_to

This specifies the email recipient for alerts.

> **Note**
>
> To use granular email configurations, a base configuration is necessary in the section.

Default value	n/a
Allowed values	Any valid email address

Use this section repeatedly for multiple email addresses, once per addresses.

email_from

This controls the “source” address in email alerts.

Default value	n/a
Allowed values	Any valid email address

email_reply_to

This controls the “reply-to” address in email alerts.

Default value	n/a
Allowed values	Any valid email address

smtp_server

This controls what SMTP server to forward email alerts to for delivery.

Default value	n/a
Allowed values	• Valid hostname or IP address. • Full path to a sendmail-like executable.

email_maxperhour

This specifies the maximum number of emails to be sent per hour. All emails in excess of this setting will be queued for later distribution.

> **Note**
>
> At the end of the hour any queued emails will be sent together in one email. This is true whether mail grouping is enabled or disabled.

Default value	12
Allowed values	Any number from 1 to 9999

email_idsname

The name will be added to the email headers with the specified value.

Default value	n/a
Allowed values	Any name

custom_alert_output

This specifies the format of alerts written to `alerts.log`. Check the allowed values for `custom_alert_output` in the following table:

Variable name	Description
$TIMESTAMP	The time the event was processed by OSSEC.
$FTELL	Unknown
$RULEALERT	Unknown
$HOSTNAME	Hostname of the system generating the event.
$LOCATION	The file the log messages was saved to.
$RULEID	The rule id of the alert.
$RULELEVEL	The rule level of the alert.
$RULECOMMENT	Unknown
$SRCIP	The source IP specified in the log message.
$DSTUSER	The destination user specified in the log message.
$FULLLOG	The original log message.
$RULEGROUP	The groups containing the rule.

stats

This controls the severity level assigned to events generated by statistical analysis.

Default value	8
Allowed values	Any level from 0 to 16

logall

This controls whether or not to store all events received even when they do not trip a rule. This results in output to /var/ossec/logs/archives/archives.log

Default value	no
Allowed values	yes or no

memory_size

This sets the memory size for the event correlation engine.

Default value	1024
Allowed values	Any size from 16 to 5096

white_list

This is a list of IP addresses that should never be blocked with active response. Repeat this option for multiple IPs, one IP per line. This option is only valid in server and local installs.

Default value	n/a
Allowed values	Any IP address or netblock

host_information

The controls the severity level for events generated by the host change monitor.

Default value	8

Allowed values	Can be used any level from 0 to 16

jsonout_output

This enables/disables writing of JSON-formated alerts to /var/ossec/logs/alerts/alerts.json. This will include the same events that would be sent to alerts.log, but in JSON format.

Default value	no
Allowed values	The options allowed are **yes** or **no**.

prelude_output

Enables or disables Prelude output.

Default value	yes
Allowed values	The options allowed are **yes** or **no**.

picviz_output

Enable PicViz output.

Default value	n/a
Allowed values	yes

picviz_socket

This is the full path of the socket that Wazuh will write alerts/events to for PicViz to read.

Default value	n/a
Allowed values	file and path that Wazuh will create and feed events to

zeromq_output

Enable ZeroMQ output.

Default value	n/a
Allowed values	The options allowed are **yes** or **no**.

zeromq_uri

This is the ZeroMQ URI that the publisher socket will bind to.

Default value	n/a
Allowed values	This URI format is defined by the ZeroMQ project.

For example, this will listen for ZeroMQ subscribers on IP address 127.0.0.1:11111.

```
<zeromq_uri>tcp://localhost:11111/</zeromq_uri>
```

This will listen on port 21212 for ZeroMQ subscribers, binding to the IP address assigned to eth0.

```
<zeromq_uri>tcp://eth0:21212/</zeromq_uri>
```

This will listen for zeromq on the Unix Domain socket /alerts-zmq.

```
<zeromq_uri>ipc:///alerts-zmq</zeromq_uri>
```

geoip_db_path

This is the full path to the MaxMind GeoIP IPv4 database file.

Default value	n/a
Allowed values	Path to the GeoIP IPv4 database file location

Example

```
<geoip_db_path>/etc/GeoLiteCity.dat</geoip_db_path>
```

Default configuration

```
<global>
  <jsonout_output>yes</jsonout_output>
  <alerts_log>yes</alerts_log>
  <logall>no</logall>
  <logall_json>no</logall_json>
  <email_notification>no</email_notification>
  <smtp_server>smtp.example.wazuh.com</smtp_server>
  <email_from>ossecm@example.wazuh.com</email_from>
  <email_to>recipient@example.wazuh.com</email_to>
  <email_maxperhour>12</email_maxperhour>
</global>
```