

integration

XML section name

```
<integration>
</integration>
```

This configures the manager to connect Wazuh to external APIs and alerting tools such as Slack and PagerDuty.

Options

- [name](#)
- [hook_url](#)
- [api_key](#)
- [level](#)
- [rule_id](#)
- [group](#)
- [event_location](#)

name

This indicates the type of the service to integrate with.

Default value	n/a
Allowed values	slack, pagerdty

hook_url

This is the URL provided by Slack when integration is enabled on the Slack side. This is **mandatory for Slack**.

Default value	n/a
Allowed values	Slack URL

api_key

This is the key that you would have retrieved from the PagerDuty API. This is **mandatory for PagerDuty**.

 **Note**

You must restart Wazuh after changing this configuration.

Default value	n/a
Allowed values	PagerDuty Api key

Optional filters

level

This filter alerts by rule level. It will push only alerts with the specified level or above.

Default value	n/a
Allowed values	Any alert level from 0 to 16

rule_id


This filters alerts by rule ID.

Default value	n/a
Allowed values	Comma-separated rule IDs

group

This filters alerts by rule group. For the VirusTotal integration, only rules from the *syscheck* group are available.

Default value	n/a
Allowed values	Any rule group or comma-separated rule groups.

 **Note**

Observe that all groups must be finished by comma.

event_location

This filters alerts by the location of where the event originated. [OS_Regex Syntax](#)

Default value	n/a
Allowed values	Any single agent name, hostname, ip address, or log file.

Example of configuration

```
<integration>
  <name>slack</name>
  <hook_url>https://hooks.slack.com/services/T000/B000/XXXXX</hook_url>
  <level>10</level>
  <group>multiple_drops,|authentication_failures,</group>
</integration>
```