

active-response

XML section name

```
<active-response>
</active-response>
```

In the active response configuration section, you bind an existing command to one or more rules or rule types and specify additional criteria for when to actually execute the command. It is possible to have as many responses as needed, but each must be in their own separate `<active-response>` section.

Options

- `disabled`
- `command`
- `location`
- `agent_id`
- `level`
- `rules_group`
- `rules_id`
- `timeout`
- `repeated_offenders`

disabled

This is a special-case option, in that it occurs alone in its own active-response section for the sole purpose of enabling or disabling the active response facility in Wazuh. In the absence of a section like this, active response is by default enabled on Unix-like systems, and disabled on Windows systems.

Setting it to `yes` on an agent will disable active-response for that agent only, while setting it in the manager’s `ossec.conf` file will disable active-response on the manager and all agents.

! Note

This option is available on server, local, and agent installations.

| | |
|----------------|--|
| Default value | no for Unix-like systems and yes for Windows systems |
| Allowed values | The options accepted are yes and no |

command

This is used to link the response to the command.

| | |
|----------------|--|
| Default value | n/a |
| Allowed values | Any defined active response command name |

location

This indicates on which system(s) the command should be executed.

| | | |
|----------------|--------|--|
| Default value | n/a | |
| Allowed values | local | This runs the command on the agent that generated the event. |
| | server | This runs the command on the Wazuh manager. |

| | | |
|--|---------------|---|
| | defined-agent | This runs the command on a specific agent identified by agent_id |
| | all | This runs the command on the Wazuh manager and on all agents. Use with caution. |

Example for `defined-agent`:

If the application that interfaces with your edge firewall runs on one of your agents, you might have a firewall-block-edge command that runs a command on that agent to blacklists an offending IP on the edge firewall.

agent_id

The ID of the agent to execute the active response command (used when defined-agent is set).

| | |
|----------------|--|
| Default value | n/a |
| Allowed values | Any agent id number, as long as defined-agent has been specified as the location. |

level


This defines a minimum severity level required for the command to be executed.

| | |
|----------------|------------------------|
| Default value | n/a |
| Allowed values | Any level from 1 to 16 |

rules_group

This requires that a rule must belong to one or more rule groups for the command to be executed.

| | |
|----------------|---|
| Default value | n/a |
| Allowed values | Any rule group is allowed. Multiple groups should be separated with a pipe character (“ ”). |

 Note

Observe that all groups must be finished by comma.

rules_id

This limits command execution to only when one or more listed rules fire.

| | |
|----------------|---|
| Default value | n/a |
| Allowed values | Any rule identification. Multiple IDs can be specified if separated by a comma. |

timeout

This specifies how long in seconds until the reverse command is executed. When `repeated_offenders` is used, `timeout` only applies to the first offense.

| | |
|----------------|-----------------------------|
| Default value | n/a |
| Allowed values | A positive number (seconds) |

repeated_offenders

This is a comma-separated list of increasing timeouts in minutes for repeat offenders. There can be a maximum of 5 entries. This must be configured directly in the **ossec.conf** file of the agent, even when using a manager/agent setup with centralized configuration of other settings via **agent.conf**.

| | |
|----------------|-----------------------------|
| Default value | n/a |
| Allowed values | A positive number (minutes) |

Example of configuration

```
<active-response>
  <disabled>no</disabled>
  <command>host-deny</command>
  <location>defined-agent</location>
  <agent-id>032</agent-id>
  <level>10</level>
  <rules_group>sshd,|pci_dss_11.4,</rules_group>
  <timeout>1</timeout>
  <repeated_offenders>1,5,10</repeated_offenders>
</active-response>
```