Reference

This API reference is organized by resources:

- Agents
- Decoders
- Manager
- Rootcheck
- Rules
- Syscheck

Also, it is provided an Request List with all available requests.

Request List

Agents

- DELETE /agents (Delete a list of agents)
- DELETE /agents/:agent_id (Delete an agent)
- GET /agents (Get all agents)
- GET /agents/:agent_id (Get an agent)
- GET /agents/:agent_id/key (Get agent key)
- GET /agents/summary (Get agents summary)
- GET /agents/summary/os (Get OS summary)
- POST /agents (Add agent)
- POST /agents/insert (Insert agent)
- POST /agents/restart (Restart a list of agents)
- PUT /agents/:agent_id/restart (Restart an agent)
- PUT /agents/:agent_name (Add agent (quick method))
- PUT /agents/restart (Restart all agents)

Decoders

- GET /decoders (Get all decoders)
- GET /decoders/:decoder_name (Get decoders by name)
- GET /decoders/files (Get all decoders files)
- GET /decoders/parents (Get all parent decoders)

Manager

- GET /manager/configuration (Get manager configuration)
- GET /manager/info (Get manager information)
- GET /manager/logs (Get ossec.log)
- GET /manager/logs/summary (Get summary of ossec.log)
- GET /manager/stats (Get manager stats)
- GET /manager/stats/hourly (Get manager stats by hour)
- GET /manager/stats/weekly (Get manager stats by week)
- GET /manager/status (Get manager status)

Rootcheck

- DELETE /rootcheck (Clear rootcheck database)
- DELETE /rootcheck/:agent_id (Clear rootcheck database of an agent)

- GET /rootcheck/:agent_id (Get rootcheck database)
- GET /rootcheck/:agent_id/cis (Get rootcheck CIS requirements)
- GET /rootcheck/:agent_id/last_scan (Get last rootcheck scan)
- GET /rootcheck/:agent_id/pci (Get rootcheck pci requirements)
- PUT /rootcheck (Run rootcheck scan in all agents)
- PUT /rootcheck/:agent_id (Run rootcheck scan in an agent)

Rules

- GET /rules (Get all rules)
- GET /rules/:rule_id (Get rules by id)
- GET /rules/files (Get files of rules)
- GET /rules/groups (Get rule groups)
- GET /rules/pci (Get rule pci requirements)

Syscheck

- DELETE /syscheck (Clear syscheck database)
- DELETE /syscheck/:agent_id (Clear syscheck database of an agent)
- GET /syscheck/:agent_id (Get syscheck files)
- GET /syscheck/:agent_id/last_scan (Get last syscheck scan)
- PUT /syscheck (Run syscheck scan in all agents)
- PUT /syscheck/:agent_id (Run syscheck scan in an agent)

Agents

Add

Add agent

Add a new agent.

Request:

`POST`

```
/agents
```

Parameters:

Param	Type	Description
`name`	String	Agent name.
ip	String	If you do not include this param, the API will get the IP automatically. If you are behind a proxy, you must set the option config.BehindProxyServer to yes at config.js. Allowed values: • IP • IP/NET • ANY
force	Number	Remove old agent with same IP if disconnected since <force> seconds.

Example Request:

```
curl -u foo:bar -k -X POST -d '{"name":"NewHost","ip":"10.0.0.9"}' -H 'Content-Type:application/json'
"https://127.0.0.1:55000/agents?pretty"
```

Example Response:

```
{
   "error": 0,
   "data": "005"
}
```

Add agent (quick method)

Adds a new agent with name :agent_name. This agent will use ANY as IP.

Request:

PUT

```
/agents/:agent_name
```

Parameters:

Param	Type	Description
`agent_name`	String	Agent name.

Example Request:

```
curl -u foo:bar -k -X PUT "https://127.0.0.1:55000/agents/myNewAgent?pretty"
```

Example Response:

```
{
   "error": 0,
   "data": "006"
}
```

Insert agent

Insert an agent with an existing id and key.

Request:

POST

```
/agents/insert
```

Parameters:

Param	Type	Description
`name`	String	Agent name.
ip	String	If you do not include this param, the API will get the IP automatically. If you are behind a proxy, you must set the option config.BehindProxyServer to yes at config.js. Allowed values: • IP • IP/NET • ANY

Param	Type	Description
`id`	String	Agent ID.
`key`	String	Agent key. Minimum length: 64 characters. Allowed values: ^[a-zA-Z0-9]+$
force	Number	Remove old agent with same IP if disconnected since <force> seconds.

Example Request:

```
curl -u foo:bar -k -X POST -d
'{"name":"NewHost_2","ip":"10.0.10.10","id":"123","key":"1abcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxy
zabcdefghi64"}' -H 'Content-Type:application/json' "https://127.0.0.1:55000/agents/insert?pretty"
```

Example Response:

```
{
   "error": 0,
   "data": "123"
}
```

Delete

Delete a list of agents

Removes a list of agents. You must restart OSSEC after removing an agent.

Request:

`DELETE`

```
/agents
```

Parameters:

Param	Type	Description
`ids`	String[]	Array of agent ID's.

Example Request:

```
curl -u foo:bar -k -X DELETE -H "Content-Type:application/json" -d '{"ids":["001","002"]}'
"https://127.0.0.1:55000/agents?pretty"
```

Example Response:

```
{
   "error": 0,
   "data": {
      "msg": "All selected agents were removed"
   }
}
```

Delete an agent

Removes an agent. You must restart OSSEC after removing an agent.

Request:

`DELETE`

```
/agents/:agent_id
```

Parameters:

Param	Type	Description
`agent_id`	Number	Agent ID.

Example Request:

```
curl -u foo:bar -k -X DELETE "https://127.0.0.1:55000/agents/002?pretty"
```

Example Response:

```
{
   "error": 0,
   "data": {
      "msg": "Some agents were not removed",
      "ids": [
         "002"
      ]
   }
}
```

Info

Get OS summary

Returns a summary of OS.

Request:

`GET`

```
/agents/summary/os
```

Parameters:

Param	Type	Description
offset	Number	First element to return in the collection.
limit	Number	Maximum number of elements to return.
sort	String	Sorts the collection by a field or fields (separated by comma). Use +/- at the beginning to ascending or descending order.
search	String	Looks for elements with the specified string.

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/agents/summary/os?pretty"
```

Example Response:

```
{
   "error": 0,
   "data": {
      "totalItems": 3,
      "items": [
         "debian",
         "ubuntu",
         "windows"
      ]
   }
}
```


Get agents summary

Returns a summary of the available agents.

Request:

`GET`

```
/agents/summary
```

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/agents/summary?pretty"
```

Example Response:


```
{
   "error": 0,
   "data": {
      "Active": 3,
      "Never connected": 3,
      "Total": 6,
      "Disconnected": 0
   }
}
```


Get all agents

Returns a list with the available agents.

Request:

`GET`

```
/agents
```

Parameters:

Param	Type	Description
offset	Number	First element to return in the collection.
limit	Number	Maximum number of elements to return.
sort	String	Sorts the collection by a field or fields (separated by comma). Use +/- at the beginning to ascending or descending order.
search	String	Looks for elements with the specified string.

Param	Type	Description
status	string	Filters by agent status. Allowed values: • active • never connected • disconnected
os.platform	String	Filters by OS platform
os.version	String	Filters by OS version

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/agents?pretty&offset=0&limit=5&sort=-ip,name"
```

Example Response:

```
{
   "error": 0,
   "data": {
      "totalItems": 6,
      "items": [
         {
            "status": "Active",
            "ip": "any",
            "os": {
               "platform": "windows",
               "version": "10.0.14393",
               "name": "Microsoft Windows Server 2016 Datacenter"
            },
            "id": "004",
            "name": "win_server"
         },
         {
            "status": "Active",
            "ip": "any",
            "os": {
               "platform": "ubuntu",
               "version": "16.04.2 LTS",
               "name": "Ubuntu"
            },
            "id": "003",
            "name": "u16"
         },
         {
            "status": "Never connected",
            "ip": "any",
            "id": "006",
            "name": "myNewAgent"
         },
         {
            "status": "Never connected",
            "ip": "10.0.10.10",
            "id": "123",
            "name": "NewHost_2"
         },
         {
            "status": "Never connected",
            "ip": "10.0.0.9",
            "id": "005",
            "name": "NewHost"
         }
      ]
   }
}
```


Get an agent

Returns the information of an agent.

Request:

`GET`

```
/agents/:agent_id
```

Parameters:

Param	Type	Description
`agent_id`	Number	Agent ID.

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/agents/000?pretty"
```

Example Response:


```
{
   "error": 0,
   "data": {
      "status": "Active",
      "name": "ip-10-0-0-10",
      "ip": "127.0.0.1",
      "dateAdd": "2017-08-05 14:47:01",
      "version": "Wazuh v2.1.0",
      "lastKeepAlive": "9999-12-31 23:59:59",
      "os": {
         "major": "8",
         "name": "Debian GNU/Linux",
         "platform": "debian",
         "uname": "Linux ip-10-0-0-10 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u2 (2016-10-19) x86_64",
         "version": "8",
         "codename": "jessie"
      },
      "id": "000"
   }
}
```


Key

Get agent key

Returns the key of an agent.

Request:

`GET`

```
/agents/:agent_id/key
```

Parameters:

Param	Type	Description
`agent_id`	Number	Agent ID.

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/agents/001/key?pretty"
```

Example Response:


```
{
   "error": 0,
   "data":
"MDAxIFdlYlNlcnZlcjEgMTAuMC4wLjYyIDNlZjEwYTQ2MGZmZDEwNDlhNDhiMmI1NjRjZmFiNGQxNmFiYzIzMzQ2NDM3MWY0ODQwZDQ0ZDJjN2RkNDkwZTE"
}
```


Restart

Restart a list of agents

Restarts a list of agents.

Request:

`POST`

```
/agents/restart
```

Parameters:

Param	Type	Description
`ids`	String[]	Array of agent ID's.

Example Request:

```
curl -u foo:bar -k -X POST -H "Content-Type:application/json" -d '{"ids":["001","002"]}'
"https://127.0.0.1:55000/agents/restart?pretty"
```

Example Response:

```
{
   "error": 0,
   "data": {
      "msg": "Some agents were not restarted",
      "ids": [
         "001",
         "002"
      ]
   }
}
```

Restart all agents

Restarts all agents.

Request:

`PUT`

```
/agents/restart
```

Example Request:

```
curl -u foo:bar -k -X PUT "https://127.0.0.1:55000/agents/restart?pretty"
```

Example Response:

```
{
    "data": "Restarting all agents",
    "error": 0
}
```

Restart an agent

Restarts the agent.

Request:

`PUT`

```
/agents/:agent_id/restart
```

Parameters:

Param	Type	Description
`agent_id`	Number	Agent unique ID.

Example Request:

```
curl -u foo:bar -k -X PUT "https://127.0.0.1:55000/agents/000/restart?pretty"
```

Example Response:

```
{
    "data": "Restarting agent",
    "error": 0
}
```

Decoders

Info

Get all decoders

Returns all decoders included in ossec.conf.

Request:

`GET`

```
/decoders
```

Parameters:

Param	Type	Description
offset	Number	First element to return in the collection.
limit	Number	Maximum number of elements to return.
sort	String	Sorts the collection by a field or fields (separated by comma). Use +/- at the beginning to ascending or descending order.
search	String	Looks for elements with the specified string.
file	String	Filters by filename.
path	String	Filters by path.
status	String	Filters the decoders by status. Allowed values: • enabled • disabled • all

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/decoders?pretty&offset=0&limit=2&sort=+file,position"
```

Example Response:


```
{
   "error": 0,
   "data": {
      "totalItems": 480,
      "items": [
         {
            "status": "enabled",
            "name": "wazuh",
            "details": {
               "prematch": "^wazuh: "
            },
            "file": "0005-wazuh_decoders.xml",
            "position": 0,
            "path": "/var/ossec/ruleset/decoders"
         },
         {
            "status": "enabled",
            "name": "agent-buffer",
            "details": {
               "regex": "^ '(\\S+)'.",
               "prematch": "^Agent buffer:",
               "parent": "wazuh",
               "order": "status"
            },
            "file": "0005-wazuh_decoders.xml",
            "position": 1,
            "path": "/var/ossec/ruleset/decoders"
         }
      ]
   }
}
```


Get all decoders files

Returns all decoders files included in ossec.conf.

Request:

`GET`

```
/decoders/files
```

Parameters:

Param	Type	Description
offset	Number	First element to return in the collection.
limit	Number	Maximum number of elements to return.
sort	String	Sorts the collection by a field or fields (separated by comma). Use +/- at the beginning to ascending or descending order.
search	String	Looks for elements with the specified string.

Param	Type	Description
status	String	Filters the decoders by status. Allowed values: • enabled • disabled • all
file	String	Filters by filename.
path	String	Filters by path.
download	String	Downloads the file

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/decoders/files?pretty&offset=0&limit=10&sort=-path"
```

Example Response:

```
{
   "error": 0,
   "data": {
      "totalItems": 85,
      "items": [
         {
            "status": "enabled",
            "path": "/var/ossec/ruleset/decoders",
            "file": "0060-cisco-estreamer_decoders.xml"
         },
         {
            "status": "enabled",
            "path": "/var/ossec/ruleset/decoders",
            "file": "0150-mysql_decoders.xml"
         },
         {
            "status": "enabled",
            "path": "/var/ossec/ruleset/decoders",
            "file": "0215-portsentry_decoders.xml"
         },
         {
            "status": "enabled",
            "path": "/var/ossec/ruleset/decoders",
            "file": "0325-suhosin_decoders.xml"
         },
         {
            "status": "enabled",
            "path": "/var/ossec/ruleset/decoders",
            "file": "0190-openvpn_decoders.xml"
         },
         {
            "status": "enabled",
            "path": "/var/ossec/ruleset/decoders",
            "file": "0405-mongodb_decoders.xml"
         },
         {
            "status": "enabled",
            "path": "/var/ossec/ruleset/decoders",
            "file": "0090-dragon-nids_decoders.xml"
         },
         {
            "status": "enabled",
            "path": "/var/ossec/ruleset/decoders",
            "file": "0085-dovecot_decoders.xml"
         },
         {
            "status": "enabled",
            "path": "/var/ossec/ruleset/decoders",
            "file": "0335-telnet_decoders.xml"
         },
         {
            "status": "enabled",
            "path": "/var/ossec/ruleset/decoders",
            "file": "0165-netscreen_decoders.xml"
         }
      ]
   }
}
```


Get all parent decoders

Returns all parent decoders included in ossec.conf

Request:

`GET`

```
/decoders/parents
```

Parameters:

Param	Type	Description
offset	Number	First element to return in the collection.
limit	Number	Maximum number of elements to return.
sort	String	Sorts the collection by a field or fields (separated by comma). Use +/- at the beginning to ascending or descending order.
search	String	Looks for elements with the specified string.

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/decoders/parents?pretty&offset=0&limit=2&sort=-file"
```

Example Response:


```
{
   "error": 0,
   "data": {
      "totalItems": 121,
      "items": [
         {
            "status": "enabled",
            "name": "local_decoder_example",
            "details": {
               "program_name": "local_decoder_example"
            },
            "file": "local_decoder.xml",
            "position": 0,
            "path": "/var/ossec/etc/decoders"
         },
         {
            "status": "enabled",
            "name": "jenkins",
            "details": {
               "prematch": "^\\w+ \\d+, \\d+ \\d+:\\d+:\\d+ \\w\\w \\S+ \\w+\\s"
            },
            "file": "0415-jenkins_decoders.xml",
            "position": 0,
            "path": "/var/ossec/ruleset/decoders"
         }
      ]
   }
}
```


Get decoders by name

Returns the decoders with the specified name.

Request:

`GET`

```
/decoders/:decoder_name
```

Parameters:

Param	Type	Description
`decoder_name`	String	Decoder name.
offset	Number	First element to return in the collection.
limit	Number	Maximum number of elements to return.
sort	String	Sorts the collection by a field or fields (separated by comma). Use +/- at the beginning to ascending or descending order.
search	String	Looks for elements with the specified string.

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/decoders/apache-errorlog?pretty"
```

Example Response:


```
{
   "error": 0,
   "data": {
      "totalItems": 3,
      "items": [
         {
            "status": "enabled",
            "name": "apache-errorlog",
            "details": {
               "program_name": "^apache2|^httpd"
            },
            "file": "0025-apache_decoders.xml",
            "position": 0,
            "path": "/var/ossec/ruleset/decoders"
         },
         {
            "status": "enabled",
            "name": "apache-errorlog",
            "details": {
               "prematch": "^[warn] |^[notice] |^[error] "
            },
            "file": "0025-apache_decoders.xml",
            "position": 1,
            "path": "/var/ossec/ruleset/decoders"
         },
         {
            "status": "enabled",
            "name": "apache-errorlog",
            "details": {
               "prematch": "^[\\w+ \\w+ \\d+ \\d+:\\d+:\\d+.\\d+ \\d+] [\\S+:warn] |^[\\w+ \\w+ \\d+
\\d+:\\d+:\\d+.\\d+ \\d+] [\\S+:notice] |^[\\w+ \\w+ \\d+ \\d+:\\d+:\\d+.\\d+ \\d+] [\\S*:error] |^[\\w+ \\w+
\\d+ \\d+:\\d+:\\d+.\\d+ \\d+] [\\S+:info] "
            },
            "file": "0025-apache_decoders.xml",
            "position": 2,
            "path": "/var/ossec/ruleset/decoders"
         }
      ]
   }
}
```


Manager

Configuration

Get manager configuration

Returns ossec.conf in JSON format.

Request:

`GET`

```
/manager/configuration
```

Parameters:

Param	Type	Description
section	String	Indicates the ossec.conf section: global, rules, syscheck, rootcheck, remote, alerts, command, active-response, localfile.
field	String	Indicates a section child, e.g, fields for rule section are: include, decoder_dir, etc.

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/manager/configuration?section=global&pretty"
```

Example Response:


```
{
   "error": 0,
   "data": {
      "email_notification": "no",
      "alerts_log": "yes",
      "jsonout_output": "yes",
      "smtp_server": "smtp.example.wazuh.com",
      "email_to": "recipient@example.wazuh.com",
      "logall": "no",
      "email_maxperhour": "12",
      "white_list": [
         "127.0.0.1",
         "^localhost.localdomain$",
         "10.0.0.2"
      ],
      "email_from": "ossecm@example.wazuh.com",
      "logall_json": "no"
   }
}
```


Info

Get manager information

Returns basic information about Manager.

Request:

`GET`

```
/manager/info
```

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/manager/info?pretty"
```

Example Response:

```
{
   "error": 0,
   "data": {
      "installation_date": "Sat Aug  5 14:46:32 UTC 2017",
      "version": "v2.1.0",
      "openssl_support": "yes",
      "max_agents": "8000",
      "ruleset_version": "v2.1.0",
      "path": "/var/ossec",
      "tz_name": "UTC",
      "type": "server",
      "tz_offset": "+0000"
   }
}
```


Get manager status

Returns the Manager processes that are running.

Request:

`GET`

```
/manager/status
```

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/manager/status?pretty"
```

Example Response:


```
{
   "error": 0,
   "data": {
      "wazuh-modulesd": "running",
      "ossec-authd": "stopped",
      "ossec-monitord": "running",
      "ossec-logcollector": "running",
      "ossec-execd": "running",
      "ossec-remoted": "running",
      "ossec-syscheckd": "running",
      "ossec-analysisd": "running",
      "ossec-maild": "stopped"
   }
}
```


Logs

Get ossec.log

Returns the 3 last months of ossec.log.

Request:

`GET`

```
/manager/logs
```

Parameters:

Param	Type	Description

Param	Type	Description
offset	Number	First element to return in the collection.
limit	Number	Maximum number of elements to return.
sort	String	Sorts the collection by a field or fields (separated by comma). Use +/- at the beginning to ascending or descending order.
search	String	Looks for elements with the specified string.
type_log	string	Filters by type of log. Allowed values: • all • error • info
category	string	Filters by category of log.

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/manager/logs?offset=0&limit=5&pretty"
```

Example Response:

```
{
    "data": {
        "totalItems": 16480,
        "items": [
            "2016/07/15 09:33:49 ossec-syscheckd: INFO: Syscheck scan frequency: 3600 seconds",
            "2016/07/15 09:33:49 ossec-syscheckd: INFO: Starting syscheck scan (forwarding database).",
            "2016/07/15 09:33:49 ossec-syscheckd: INFO: Starting syscheck database (pre-scan).",
            "2016/07/15 09:33:42 ossec-logcollector: INFO: Started (pid: 2832).",
            "2016/07/15 09:33:42 ossec-logcollector: INFO: Monitoring output of command(360): df -P"
        ]
    },
    "error": 0
}
```

Get summary of ossec.log

Returns a summary about the 3 last months of ossec.log.

Request:

`GET`

```
/manager/logs/summary
```

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/manager/logs/summary?pretty"
```

Example Response:

```
{
   "error": 0,
   "data": {
      "wazuh-modulesd": {
         "info": 2,
         "all": 2,
         "error": 0
      },
      "ossec-testrule": {
         "info": 172,
         "all": 172,
         "error": 0
      },
      "wazuh-modulesd:oscap": {
         "info": 2,
         "all": 2,
         "error": 0
      },
      "ossec-rootcheck": {
         "info": 6,
         "all": 6,
         "error": 0
      },
      "ossec-monitord": {
         "info": 3,
         "all": 3,
         "error": 0
      },
      "ossec-logcollector": {
         "info": 25,
         "all": 27,
         "error": 2
      },
      "ossec-execd": {
         "info": 4,
         "all": 4,
         "error": 0
      },
      "ossec-remoted": {
         "info": 416,
         "all": 1047,
         "error": 631
      },
      "ossec-syscheckd": {
         "info": 51,
         "all": 51,
         "error": 0
      },
      "ossec-analysisd": {
         "info": 389,
         "all": 389,
         "error": 0
      },
      "wazuh-modulesd:database": {
         "info": 2,
         "all": 2,
         "error": 0
      }
   }
}
```


Stats

Get manager stats

Returns OSSEC statistical information of current date.

Request:

`GET`

```
/manager/stats
```

Parameters:

Param	Type	Description
date	String	Selects the date for getting the statistical information. Format: YYYYMMDD

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/manager/stats?pretty"
```

Example Response:

```
{
    "data": [
        {
            "hour": 5,
            "firewall": 0,
            "alerts": [
                {
                    "level": 3,
                    "sigid": 5715,
                    "times": 4
                },
                {
                    "level": 2,
                    "sigid": 1002,
                    "times": 2
                },
                {
                    "...": "..."
                }
            ],
            "totalAlerts": 107,
            "syscheck": 1257,
            "events": 1483
        },
        {
            "...": "..."
        }
    ],
    "error": 0
}
```

Get manager stats by hour

Returns OSSEC statistical information per hour. Each item in averages field represents the average of alerts per hour.

Request:

`GET`

```
/manager/stats/hourly
```

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/manager/stats/hourly?pretty"
```

Example Response:


```
{
    "data": {
        "averages": [
            100,
            357,
            242,
            500,
            422,
            "...",
            123
        ],
        "interactions": 0
    },
    "error": 0
}
```


Get manager stats by week

Returns OSSEC statistical information per week. Each item in hours field represents the average of alerts per hour and week day.

Request:

`GET`

```
/manager/stats/weekly
```

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/manager/stats/weekly?pretty"
```

Example Response:

```
{
    "data": {
        "Wed": {
            "hours": [
                223,
                "...",
                456
            ],
            "interactions": 0
        },
        "Sun": {
            "hours": [
                332,
                "...",
                313
            ],
            "interactions": 0
        },
        "Thu": {
            "hours": [
                888,
                "...",
                123
            ],
            "interactions": 0
        },
        "Tue": {
            "hours": [
                536,
                "...",
                345
            ],
            "interactions": 0
        },
        "Mon": {
            "hours": [
                444,
                "...",
                556
            ],
            "interactions": 0
        },
        "Fri": {
            "hours": [
                131,
                "...",
                432
            ],
            "interactions": 0
        },
        "Sat": {
            "hours": [
                134,
                "...",
                995
            ],
            "interactions": 0
        }
    },
    "error": 0
}
```


Rootcheck

Clear

Clear rootcheck database

Clears the rootcheck database for all agents.

Request:

`DELETE`

```
/rootcheck
```

Example Request:

```
curl -u foo:bar -k -X DELETE "https://127.0.0.1:55000/rootcheck?pretty"
```

Example Response:

```
{
    "data": "Rootcheck database deleted",
    "error": 0
}
```

Clear rootcheck database of an agent

Clears the rootcheck database for an agent.

Request:

`DELETE`

```
/rootcheck/:agent_id
```

Parameters:

Param	Type	Description
`agent_id`	Number	Agent ID.

Example Request:

```
curl -u foo:bar -k -X DELETE "https://127.0.0.1:55000/rootcheck/000?pretty"
```

Example Response:

```
{
    "data": "Rootcheck database deleted",
    "error": 0
}
```

Info

Get last rootcheck scan

Return the timestamp of the last rootcheck scan.

Request:

`GET`

```
/rootcheck/:agent_id/last_scan
```

Parameters:

Param	Type	Description
`agent_id`	Number	Agent ID.

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/rootcheck/000/last_scan?pretty"
```

Example Response:


```
{
   "error": 0,
   "data": {
      "start": "2017-08-05 14:48:07",
      "end": "2017-08-05 14:47:33"
   }
}
```


Get rootcheck CIS requirements

Returns the CIS requirements of all rootchecks of the agent.

Request:

`GET`

```
/rootcheck/:agent_id/cis
```

Parameters:

Param	Type	Description
offset	Number	First element to return in the collection.
limit	Number	Maximum number of elements to return.
sort	String	Sorts the collection by a field or fields (separated by comma). Use +/- at the beginning to ascending or descending order.
search	String	Looks for elements with the specified string.

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/rootcheck/000/cis?offset=0&limit=10&pretty"
```

Example Response:


```
{
   "error": 0,
   "data": {
      "totalItems": 2,
      "items": [
         "1.4 Debian Linux",
         "4.13 Debian Linux"
      ]
   }
}
```

Get rootcheck database

Returns the rootcheck database of an agent.

Request:

`GET`

```
/rootcheck/:agent_id
```

Parameters:

Param	Type	Description
`agent_id`	Number	Agent ID.
pci	String	Filters by pci requirement.
cis	String	Filters by CIS.
offset	Number	First element to return in the collection.
limit	Number	Maximum number of elements to return.
sort	String	Sorts the collection by a field or fields (separated by comma). Use +/- at the beginning to ascending or descending order.
search	String	Looks for elements with the specified string.

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/rootcheck/000?offset=0&limit=2&pretty"
```

Example Response:

```
{
   "error": 0,
   "data": {
      "totalItems": 8,
      "items": [
         {
            "status": "outstanding",
            "oldDay": "2017-08-05 14:47:18",
            "readDay": "2017-08-05 14:48:08",
            "event": "File '/var/lib/test' is owned by root and has written permissions to anyone."
         },
         {
            "status": "outstanding",
            "oldDay": "2017-08-05 14:47:18",
            "cis": "1.4 Debian Linux",
            "readDay": "2017-08-05 14:48:07",
            "event": "System Audit: CIS - Debian Linux - 1.4 - Robust partition scheme - /opt is not on its
own partition {CIS: 1.4 Debian Linux}. File: /opt. Reference:
https://benchmarks.cisecurity.org/tools2/linux/CIS_Debian_Benchmark_v1.0.pdf ."
         }
      ]
   }
}
```

Get rootcheck pci requirements

Returns the PCI requirements of all rootchecks of the agent.

Request:

`GET`

```
/rootcheck/:agent_id/pci
```

Parameters:

Param	Type	Description
offset	Number	First element to return in the collection.
limit	Number	Maximum number of elements to return.
sort	String	Sorts the collection by a field or fields (separated by comma). Use +/- at the beginning to ascending or descending order.
search	String	Looks for elements with the specified string.

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/rootcheck/000/pci?offset=0&limit=10&pretty"
```

Example Response:

```
{
   "error": 0,
   "data": {
      "totalItems": 2,
      "items": [
         "2.2.2",
         "2.2.4"
      ]
   }
}
```

Run

Run rootcheck scan in all agents

Runs syscheck and rootcheck on all agent, due to OSSEC launches both processes at once.

Request:

PUT

```
/rootcheck
```

Example Request:

```
curl -u foo:bar -k -X PUT "https://127.0.0.1:55000/rootcheck?pretty"
```

Example Response:

```
{
    "data": "Restarting Syscheck/Rootcheck on all agents",
    "error": 0
}
```

Run rootcheck scan in an agent

Runs syscheck and rootcheck on an agent, due to OSSEC launches both processes at once.

Request:

`PUT`

```
/rootcheck/:agent_id
```

Parameters:

Param	Type	Description
`agent_id`	Number	Agent ID.

Example Request:

```
curl -u foo:bar -k -X PUT "https://127.0.0.1:55000/rootcheck/000?pretty"
```

Example Response:

```
{
   "error": 0,
   "data": "Restarting Syscheck/Rootcheck locally"
}
```

Rules

Info

Get all rules

Returns all rules.

Request:

`GET`

```
/rules
```

Parameters:

Param	Type	Description
offset	Number	First element to return in the collection.
limit	Number	Maximum number of elements to return.
sort	String	Sorts the collection by a field or fields (separated by comma). Use +/- at the beginning to ascending or descending order.
search	String	Looks for elements with the specified string.
status	String	Filters the rules by status. Allowed values: • enabled • disabled • all
group	String	Filters the rules by group.
level	Range	Filters the rules by level. level=2 or level=2-5.
path	String	Filters the rules by path.

Param	Type	Description
file	String	Filters the rules by file name.
pci	String	Filters the rules by pci requirement.

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/rules?offset=0&limit=2&pretty"
```

Example Response:


```
{
   "error": 0,
   "data": {
      "totalItems": 1701,
      "items": [
         {
            "status": "enabled",
            "pci": [],
            "description": "Generic template for all syslog rules.",
            "file": "0010-rules_config.xml",
            "level": 0,
            "path": "/var/ossec/ruleset/rules",
            "groups": [
               "syslog"
            ],
            "id": 1,
            "details": {
               "category": "syslog",
               "noalert": "1"
            }
         },
         {
            "status": "enabled",
            "pci": [],
            "description": "Generic template for all firewall rules.",
            "file": "0010-rules_config.xml",
            "level": 0,
            "path": "/var/ossec/ruleset/rules",
            "groups": [
               "firewall"
            ],
            "id": 2,
            "details": {
               "category": "firewall",
               "noalert": "1"
            }
         }
      ]
   }
}
```


Get files of rules

Returns the files of all rules.

Request:

`GET`

```
/rules/files
```

Parameters:

Param	Type	Description
offset	Number	First element to return in the collection.
limit	Number	Maximum number of elements to return.
sort	String	Sorts the collection by a field or fields (separated by comma). Use +/- at the beginning to ascending or descending order.
search	String	Looks for elements with the specified string.
status	String	Filters files by status. Allowed values: • enabled • disabled • all
path	String	Filters the rules by path.
file	String	Filters the rules by filefile.
download	String	Downloads the file

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/rules/files?offset=0&limit=10&pretty"
```

Example Response:

```
{
   "error": 0,
   "data": {
      "totalItems": 95,
      "items": [
         {
            "status": "enabled",
            "path": "/var/ossec/ruleset/rules",
            "file": "0010-rules_config.xml"
         },
         {
            "status": "enabled",
            "path": "/var/ossec/ruleset/rules",
            "file": "0015-ossec_rules.xml"
         },
         {
            "status": "enabled",
            "path": "/var/ossec/ruleset/rules",
            "file": "0016-wazuh_rules.xml"
         },
         {
            "status": "enabled",
            "path": "/var/ossec/ruleset/rules",
            "file": "0020-syslog_rules.xml"
         },
         {
            "status": "enabled",
            "path": "/var/ossec/ruleset/rules",
            "file": "0025-sendmail_rules.xml"
         },
         {
            "status": "enabled",
            "path": "/var/ossec/ruleset/rules",
            "file": "0030-postfix_rules.xml"
         },
         {
            "status": "enabled",
            "path": "/var/ossec/ruleset/rules",
            "file": "0035-spamd_rules.xml"
         },
         {
            "status": "enabled",
            "path": "/var/ossec/ruleset/rules",
            "file": "0040-imapd_rules.xml"
         },
         {
            "status": "enabled",
            "path": "/var/ossec/ruleset/rules",
            "file": "0045-mailscanner_rules.xml"
         },
         {
            "status": "enabled",
            "path": "/var/ossec/ruleset/rules",
            "file": "0050-ms-exchange_rules.xml"
         }
      ]
   }
}
```


Get rule groups

Returns the groups of all rules.

Request:

`GET`

```
/rules/groups
```

Parameters:

Param	Type	Description
offset	Number	First element to return in the collection.
limit	Number	Maximum number of elements to return.
sort	String	Sorts the collection by a field or fields (separated by comma). Use +/- at the beginning to ascending or descending order.
search	String	Looks for elements with the specified string.

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/rules/groups?offset=0&limit=10&pretty"
```

Example Response:


```
{
   "error": 0,
   "data": {
      "totalItems": 242,
      "items": [
         "access_control",
         "access_denied",
         "accesslog",
         "account_changed",
         "active_response",
         "adduser",
         "agent",
         "agent_flooding",
         "agentless",
         "amazon"
      ]
   }
}
```


Get rule pci requirements

Returns the PCI requirements of all rules.

Request:

`GET`

```
/rules/pci
```

Parameters:

Param	Type	Description
offset	Number	First element to return in the collection.
limit	Number	Maximum number of elements to return.
sort	String	Sorts the collection by a field or fields (separated by comma). Use +/- at the beginning to ascending or descending order.
search	String	Looks for elements with the specified string.

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/rules/pci?offset=0&limit=10&pretty"
```

Example Response:


```
{
   "error": 0,
   "data": {
      "totalItems": 38,
      "items": [
         "1.1.1",
         "1.3.4",
         "1.4",
         "10.1",
         "10.2.1",
         "10.2.2",
         "10.2.4",
         "10.2.5",
         "10.2.6",
         "10.2.7"
      ]
   }
}
```


Get rules by id

Returns the rules with the specified id.

Request:

`GET`

```
/rules/:rule_id
```

Parameters:

Param	Type	Description
`id`	Number	rule.
offset	Number	First element to return in the collection.
limit	Number	Maximum number of elements to return.
sort	String	Sorts the collection by a field or fields (separated by comma). Use +/- at the beginning to ascending or descending order.
search	String	Looks for elements with the specified string.

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/rules/1002?pretty"
```

Example Response:

```
{
   "error": 0,
   "data": {
      "totalItems": 1,
      "items": [
         {
            "status": "enabled",
            "pci": [],
            "description": "Unknown problem somewhere in the system.",
            "file": "0020-syslog_rules.xml",
            "level": 2,
            "path": "/var/ossec/ruleset/rules",
            "groups": [
               "syslog",
               "errors"
            ],
            "id": 1002,
            "details": {
               "options": "alert_by_email",
               "match": "$BAD_WORDS"
            }
         }
      ]
   }
}
```


Syscheck

Clear

Clear syscheck database

Clears the syscheck database for all agents.

Request:

`DELETE`

```
/syscheck
```

Example Request:

```
curl -u foo:bar -k -X DELETE "https://127.0.0.1:55000/syscheck?pretty"
```

Example Response:


```
{
    "data": "Syscheck database deleted",
    "error": 0
}
```


Clear syscheck database of an agent

Clears the syscheck database for an agent.

Request:

`DELETE`

```
/syscheck/:agent_id
```

Parameters:

Param	Type	Description
`agent_id`	Number	Agent ID.

Example Request:

```
curl -u foo:bar -k -X DELETE "https://127.0.0.1:55000/syscheck/000?pretty"
```

Example Response:

```
{
    "data": "Syscheck database deleted",
    "error": 0
}
```

Info

Get last syscheck scan

Return the timestamp of the last syscheck scan.

Request:

`GET`

```
/syscheck/:agent_id/last_scan
```

Parameters:

Param	Type	Description
`agent_id`	Number	Agent ID.

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/syscheck/000/last_scan?pretty"
```

Example Response:

```
{
   "error": 0,
   "data": {
      "start": "2017-08-05 14:48:04",
      "end": "2017-08-05 14:48:07"
   }
}
```

Get syscheck files

Returns the syscheck files of an agent.

Request:

`GET`

```
/syscheck/:agent_id
```

Parameters:

Param	Type	Description
`agent_id`	Number	Agent ID.
offset	Number	First element to return in the collection.
limit	Number	Maximum number of elements to return.
sort	String	Sorts the collection by a field or fields (separated by comma). Use +/- at the beginning to ascending or descending order.
search	String	Looks for elements with the specified string.
event	String	Filters files by event. Allowed values: • added • readded • modified • deleted
file	String	Filters file by filename.
filetype	String	Selects type of file. Allowed values: • file • registry
summary	String	Returns a summary grouping by filename. Allowed values: • yes • no
md5	String	Returns the files with the specified md5 hash.
sha1	String	Returns the files with the specified sha1 hash.
hash	String	Returns the files with the specified hash (md5 or sha1).

Example Request:

```
curl -u foo:bar -k -X GET "https://127.0.0.1:55000/syscheck/000?offset=0&limit=2&pretty"
```

Example Response:

```
{
   "error": 0,
   "data": {
      "totalItems": 0,
      "items": []
   }
}
```

Run

Run syscheck scan in all agents

Runs syscheck and rootcheck on all agent, due to OSSEC launches both processes at once.

Request:

`PUT`

```
/syscheck
```

Example Request:

```
curl -u foo:bar -k -X PUT "https://127.0.0.1:55000/syscheck?pretty"
```

Example Response:

```
{
    "data": "Restarting Syscheck/Rootcheck on all agents",
    "error": 0
}
```

Run syscheck scan in an agent

Runs syscheck and rootcheck on an agent, due to OSSEC launches both processes at once.

Request:

`PUT`

```
/syscheck/:agent_id
```

Parameters:

Param	Type	Description
`agent_id`	Number	Agent ID.

Example Request:

```
curl -u foo:bar -k -X PUT "https://127.0.0.1:55000/syscheck/000?pretty"
```

Example Response:

```
{
   "error": 0,
   "data": "Restarting Syscheck/Rootcheck locally"
}
```