EclecticIQ Intelligence at the core

Intelligence Hunting Response

EclecticIQ Endpoint Response REST API Guide

Version 4.0.0

October 2022

Table of contents

Getting started

The EclecticIQ Endpoint Response platform is a sophisticated and flexible endpoint monitoring and response platform. It provides endpoint monitoring and visibility, threat detection, and incident response for Security Operating Centers (SOCs).

EclecticIQ Endpoint Response REST APIs allow developers to use a programming language of their choice to integrate with the headless EclecticIQ Endpoint Response server. The REST APIs allow you to configure and query the data from the fleet manager. All payloads are exchanged over REST and use the JSON schema.

The REST-based APIs:

- Make use of standard HTTP verbs, such a GET, POST, DELETE
- Use standard HTTP error responses to detail errors
- Provide authentication using API keys in the HTTP Authorization header
- Send requests and responses in JSON format

Intended audience

This document is intended to help developers, engineers, and support staff to use APIs to integrate with the headless EclecticIQ Endpoint Response server. This guide details APIs for the Enterprise Edition and Community Edition of EclecticIQ Endpoint Response.

Terminology used in this guide

Term	***Description***
Fleet	Refers to a set of endpoints that are running the EclecticIQ Endpoint Response agent and are managed by the EclecticIQ Endpoint Response server.
Node	Represents a specific endpoint that is actively monitored.
Config	EclecticIQ Endpoint Response osquery-based agent derives its behavior from its configuration. The config is a JSON file that includes options used to control agent behavior and specifies queries scheduled on the agent. Config is applied at a node level. For more information on the configuration, refer to the *EclecticIQ Endpoint Response Deployment Guide*.
Options	Options (or flags) are parameters that the agent uses to influence its behavior. A list of all supported flags can be found here. Options can also be modified as part of config.
Tag	A mechanism to logically group or associate elements, such as nodes, packs, and queries.

Scheduled Query	Queries that run on a specified schedule on one or more endpoints.
Query Pack	A group of scheduled queries.
Ad Hoc Query	A live and on-demand query that is targeted at an endpoint or a set of endpoints. This is also referred to as a distributed query.
Alerts	Rules can be applied to the results of scheduled queries. When events match with a rule, the EclecticIQ Endpoint Response server generates an alert with the event information for proactive analysis by SOC analysts.
Active Response	Actions that can be taken on one or more affected endpoints. This is available only in the Enterprise Edition of EclecticIQ Endpoint Response and unavailable in the Community Edition.

About the APIs

This section provides generic information about the EclecticIQ Endpoint Response REST APIs.

Versioning

EclecticIQ Endpoint Response APIs are versioned. EclecticIQ reserves the right to add new parameters, properties, or resources to the APIs without advance notice. These updates are considered non-breaking, and the compatibility rules below should be followed to ensure your application does not break.

Breaking or major changes, such as removing or renaming an attribute will be released as an updated version of the API. EclecticIQ will provide a migration path for new versions of APIs and will communicate timelines for end-of-life when deprecating APIs. Do not consume any API unless it is formally documented. All undocumented endpoints should be considered private, subject to change without notice, and not covered by any agreements.

The API version is currently v1. All API requests must use the HTTPS scheme.

BASE_URL

API calls are made to a URL to identify the location from which the data is accessed. You must replace the placeholders `<server_IP>` with actual details of your EclecticIQ Endpoint Response server. The BASE_URL follows this syntax:

```
https://<server_IP>/esp-ui/services/api/v1
```

Authentication

The EclecticIQ Endpoint Response APIs require all requests to present a valid API key (x-access-token: API Key) specified in the HTTP Authorization header for every HTTP request. While logging in

(`<BASE_URL>/login`) the x-access-token is provided from the server, which needs to be used for further API calls. If the API key is missing or invalid, a 401 unauthorized response code is returned.

The API key (x-access-token) has the privileges associated with an administrator account. The API key cannot be used to authenticate once the user logs out from the platform or the default expiry time (7 days is set for now) is reached. If you believe your API key is compromised or expired, you can generate a new one. This ensures that the older API key can no longer be used to authenticate to the server.

x-access-token

The EclecticIQ ESP server provides an authentication token called x-access-token, which is an encoded JSON web token (JWT) and is used as a unique key for all future API calls. The x-access-token is provided at the URL `<BASE_URL>/login`.

Transport security

HTTP over TLS v1.2 is enforced for all API calls. The EclecticIQ Endpoint Response server rejects all non-secure calls.

Client request context

EclecticIQ Endpoint Response derives the client request context directly from the HTTP request header and client TCP socket. Request context is used to evaluate policies and provide client information for troubleshooting and auditing purposes.

User agent	The EclecticIQ Endpoint Response server supports the standard user-agent HTTP header to identify the client application. Always send a user-agent string to uniquely identify your client application and version, such as SOC Application/1.1.
IP address	The IP address of your application is automatically used as the client IP address for your request.

Common error codes

On success, all requests return a 200 status if there is content to return or a 204 status if there is no content to return.

The following HTTP response codes are used to indicate API errors.

Code	***Description***
400	Malformed or bad JSON request
401	API access without authentication or with invalid API key
403	User doesn't have access to the resource

404	Resource not found
410	Resource unavailable
422	Request parsed but includes invalid content
429	Too many requests; server has reached its limit
200	Success
201	Created (returned after a successful POST request, after a resource is created)
500	Internal server error
503	Service currently unavailable

REST API header details

Here are the headers required in the REST API.

Category	***Header details***

For POST method (except /login)	`{`
	`  "Content-Type": "application/json",`
	`  "x-access-token": "<received from /login API>"`
	`}`

For GET method	`{`
	`  "x-access-token": "<received from /login API>"`
	`}`

For /login API	`{`
	`  "Content-Type": "application/json"`
	`}`

For all APIs with files in the payload	`{`
	`  "Content-Type": "multipart/form-data",`
	`  "x-access-token": "<received from /login API>"`
	`}`

Download the certificate and client installer

Use this API to download the download the following:

- Certificate
- Client installer for Windows, Linux, and macOS

URL format

Task	***URL format***
To download the certificate	`https://<server_IP>/downloads/certificate.crt`
To download the Windows Client Provisioning Tool	`https://<server_IP>/downloads/windows/plgx_cpt.exe`
To download the Linux Client Provisioning Tool	`https://<server_IP>/downloads/linux/plgx_cpt`
To download the macOS installer	`https://<server_IP>/downloads/plgx_cpt.sh`

Request type

GET

Get dashboard data

Use this API to fetch all the data needed for EclecticIQ Endpoint Response server dashboard.

URL

/dashboard

Request type

GET

Example response format


```
{
  "status": "success",
  "message": "Data is fetched successfully",
  "data": {
    "alert_data": {
      "top_five": {
        "rule": [
          {
            "rule_id": 147,
            "rule_name": "Windows Defender Anti-Malware Alerts",
            "count": 6
          }
        ],
        "hosts": [
```

```
      {
        "host_id": 13,
        "host_identifier": "EXAMPLEHOSTIDENTIFIER",
        "host_name": "EXAMPLEHOST",
        "count": 31
      }
    ],
    "query": [
      {
        "query_name": "windows_real_time_events",
        "count": 53
      }
    ]
  },
  "source": {
    "ioc": {
      "INFO": 0,
      "LOW": 0,
      "MEDIUM": 45,
      "CRITICAL": 0,
      "HIGH": 0,
      "TOTAL": 45
    },
    "rule": {
      "INFO": 1,
      "LOW": 0,
      "MEDIUM": 0,
      "CRITICAL": 0,
      "HIGH": 0,
      "TOTAL": 8
    },
    "virustotal": {
      "INFO": 0,
      "LOW": 0,
      "MEDIUM": 0,
      "CRITICAL": 0,
      "HIGH": 0,
      "TOTAL": 0
    },
    "ibmxforce": {
      "INFO": 0,
      "LOW": 0,
      "MEDIUM": 0,
      "CRITICAL": 0,
      "HIGH": 0,
      "TOTAL": 0
    },
    "alienvault": {
      "INFO": 0,
      "LOW": 0,
      "MEDIUM": 0,
      "CRITICAL": 0,
```

```
          "HIGH": 0,
          "TOTAL": 0
        }
      }
    },
    "purge_duration": "7",
    "distribution_and_status": {
      "hosts_platform_count": [
        {
          "os_name": "darwin",
          "count": 1
        },
        {
          "os_name": "ubuntu",
          "count": 3
        },
        {
          "os_name": "windows",
          "count": 9
        }
      ],
      "hosts_status_count": {
        "online": 0,
        "offline": 13
      }
    }
  }
}
```


Authentication

This section details the various APIs available for authentication.

Get authentication metadata

Use this API to fetch password or SSO login information.

URL

/index

Request type

GET

Example response format


```
{
  "sso_status": true
}
```

Get authentication token

Use this API to fetch the authentication token that can be used in future API requests.

URL

/login

Request type

POST

Example payload format

```
{
  "username": "foo",
  "password": "Foobar123#"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
username	Required	String	Username of the platform user.
password	Required	String	Password of the platform user.

Example response format

```
{
  "all_roles": "admin,analyst",
  "auth_type": "password",
  "first_name": "",
  "last_name": "",
  "reset_email": true,
  "reset_password": false,
  "roles": "admin",
  "token":
"eyJhbGciOiJIUzUxMiIsImlhdCI6MTY0Mzk1ODAwMSwiZXhwIjoxNjQ0NTYyODAxfQ.ey
JpZCI6MX0.2JXsc1INNbDqvh9XRLw54MGkTB3hOT-B7H33Y0nP0UqI9wsIHmiiP-
I47MtbyA2FJU7cMZqtYyvAOLYQVr69Pw"
}
```

Terminate the authentication token

Use this API to make the auth token (x-access-token) invalid so that it cannot be used for authenticating APIs.

URL

/logout

Request type

POST

Example response format:

```
{
  "message": "user logged out successfully",
  "status": "success"
}
```

Initiate SSO authentication

Use this API to initiate the SSO (SAML) authentication.

URL

/sso/login

Request type

GET

Example response format

Response 302 - Redirect response to provided IDP URL

Initiate SSO callback

After successful identity validation, use the API for the IDP (Identity provider) to call. The auth token and other metadata are saved in the local storage of the browser.

URL

/sso/callback

Request type

POST

Example payload format

```
{
  "SAMLResponse": "<SAML JWT Token from IDP>"
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
SAMLResponse	Required	String	JWT encoded Security Assertion Markup Language (SAML) token from the IDP.

Hosts

This section describes APIs that help in host management.

Get a list of all hosts

Use this API to fetch a list of hosts that can be filtered based on the search or filter parameters.

URL

/hosts

Request type

POST

Example payload format

```
{
  "start": 0,
  "limit": 25,
  "searchterm": ""
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
status	Optional	Boolean	Specifies whether to fetch information for online or offline hosts. • Specify a value of true to fetch only online hosts • Specify a value of false to fetch only offline hosts
platform	Optional	String	Specifies the operating system to filter the fetched hosts. Possible values are windows, linux, and darwin. If a value is specified, returns only hosts for the specified platform.
enabled	Optional	Boolean	Specifies whether to fetch information for active or inactive hosts. • Specify a value of true to fetch information for active hosts. • Specify a value of false to fetch information for removed hosts. By default, this is set to null returning information for both active and inactive hosts.
alerts_count	Optional	Boolean	Indicates it alert count is provided for each host. Specify a value of true to fetch alert count for the host. By default, this is set to true.

start	Optional	integer	Specifies the start value of the results. This value is use for pagination. By default, this is set to 0.
limit	Optional	integer	Specifies the end value of the results. This value is use for pagination. By default, this is set to 10.
searchterm	Optional	string	Specifies the term to filter the search results. Only results containing the searchterm are returned.
column	Optional	String	Specifies the name of the column based on which to sort the results. This is used in conjunction with order_by. Possible values are host, state, health, os, and last_ip.
order_by	Optional	String	Specifies how to sort the results. This is used in conjunction with column. Possible values are asc (for ascending) and desc (for descending).

Example response format


```
{
  "status": "success",
  "message": "Successfully fetched the hosts details",
  "data": {
    "results": [
      {
        "id": 13,
        "display_name": "EXAMPLEHOST",
        "host_identifier": "EXAMPLEHOSTIDENTIFIER",
        "os_info": {
          "arch": "64-bit",
          "name": "Microsoft Windows Server 2019 Datacenter",
          "build": "17763",
          "major": "10",
          "minor": "0",
          "patch": "",
          "version": "10.0.17763",
          "codename": "Microsoft Windows Server 2019 Datacenter",
          "platform": "windows",
          "install_date": "1614737973",
          "platform_like": "windows"
        },
        "tags": [
          "foo"
```

```
        ],
        "last_ip": "13.0.0.13",
        "is_active": true,
        "alerts_count": 31
      }
    ],
    "count": 13,
    "total_count": 13
  }
}
```


Export selected hosts

Use the API to export a list of hosts (filtered based on the search or filter parameters) to a CSV file.

URL

/hosts/export

Request type

POST

Example payload format


```
{
  "start": 0,
  "limit": 25,
  "searchterm": ""
}
```


Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
status	Optional	Boolean	Specifies whether to fetch information for online or offline hosts. • Specify a value of true to fetch only online hosts • Specify a value of false to fetch only offline hosts
platform	Optional	String	Specifies the operating system to filter the fetched hosts. Possible values are windows, linux, and darwin. If a value is specified, returns only hosts for the specified platform.
enabled	Optional	Boolean	Specifies whether to fetch information for active or inactive hosts. • Specify a value of true to fetch information for active hosts.

			• Specify a value of false to fetch information for removed hosts. By default, this is set to null returning information for both active and inactive hosts.
alerts_count	Optional	Boolean	Indicates it alert count is provided for each host. Specify a value of true to fetch alert count for the host. By default, this is set to true.
start	Optional	integer	Specifies the start value of the results. This value is use for pagination. By default, this is set to 0.
limit	Optional	integer	Specifies the end value of the results. This value is use for pagination. By default, this is set to 10.
searchterm	Optional	string	Specifies the term to filter the search results. Only results containing the searchterm are returned.
column	Optional	String	Specifies the name of the column based on which to sort the results. This is used in conjunction with order_by. Possible values are host, state, health, os, and last_ip.
order_by	Optional	String	Specifies how to sort the results. This is used in conjunction with column. Possible values are asc (for ascending) and desc (for descending).

Export all hosts

Use the API to export all the hosts (and their metadata) to a CSV file.

URL

/hosts/export

Request type

GET

Get information for a host

Use this API to fetch information (and metadata) for a specific host by providing host ID.

URL

/hosts/<node id>

Request type

GET

Example response format


```
{
  "status": "success",
  "message": "Node details are fetched successfully",
  "data": {
    "id": 13,
    "host_identifier": "EXAMPLEHOSTIDENTIFIER",
    "node_key": "example-node-key",
    "last_ip": "13.0.0.13",
    "platform": "windows",
    "os_info": {
      "arch": "64-bit",
      "name": "Microsoft Windows Server 2019 Datacenter",
      "build": "17763",
      "major": "10",
      "minor": "0",
      "patch": "",
      "version": "10.0.17763",
      "codename": "Microsoft Windows Server 2019 Datacenter",
      "platform": "windows",
      "install_date": "1614737973",
      "platform_like": "windows"
    },
    "node_info": {
      "computer_name": "EXAMPLEHOST",
      "hardware_model": "HVM domU",
      "hardware_serial": "example-serial-number",
      "hardware_vendor": "Xen",
      "physical_memory": "8589524992",
      "cpu_physical_cores": "2"
    },
    "network_info": [
      {
        "mac": "02:09:d9:23:7a:0a",
        "mask": "ffff:ffff:ffff:ffff::",
        "address": "fe80::ac17:d5a5:bf91:63",
        "enabled": "1",
        "description": "AWS PV Network Device #0",
        "manufacturer": "Amazon Inc.",
        "connection_id": "Ethernet",
        "connection_status": "2"
      }
```

```
    ],
    "host_details": {
      "osquery_info": {
        "pid": "512",
        "uuid": "EXAMPLEHOSTIDENTIFIER",
        "version": "4.7.0",
        "watcher": "6600",
        "extensions": "active",
        "start_time": "1643869945",
        "config_hash": "f80dee827635db39077a458243379b3ad63311fd",
        "instance_id": "d7150e91-b22e-42a5-bde4-9bf1fec76965",
        "build_distro": "10",
        "config_valid": "1",
        "platform_mask": "2",
        "build_platform": "windows"
      },
      "osquery_version": "4.7.0",
      "extension_version": "3.5.0"
    },
    "last_checkin": "2022-02-03T09:40:55.689631",
    "enrolled_on": "2022-02-03T06:32:34.974071",
    "last_status": "2022-02-03T07:15:42.140530",
    "last_result": "2022-02-03T09:40:55.689629",
    "last_config": "2022-02-03T07:36:29.593267",
    "last_query_read": "2022-02-03T09:07:25.406080",
    "last_query_write": "2022-02-03T09:07:25.465264"
  }
}
```


Get alert distribution for a host

Use this API to retrieve alert distribution for a host based on alert sources and rules.

All alerts received for the host are categorized based on the source, such as IOC, rules, VirusTotal, IBMxForce, and AlienVault. For rule information, this API fetches top five rules generating most alerts for the host.

URL

/hosts/<node_id>/alerts/distribution

Request type

GET

Example response format


```
{
  "status": "success",
  "message": "Alerts distribution details are fetched for the host",
  "data": {
    "sources": {
      "ioc": {
        "INFO": 0,
```

```
          "LOW": 0,
          "MEDIUM": 24,
          "CRITICAL": 0,
          "HIGH": 0,
          "TOTAL": 24
        },
        "rule": {
          "INFO": 0,
          "LOW": 0,
          "MEDIUM": 0,
          "CRITICAL": 7,
          "HIGH": 0,
          "TOTAL": 7
        },
        "virustotal": {
          "INFO": 0,
          "LOW": 0,
          "MEDIUM": 0,
          "CRITICAL": 0,
          "HIGH": 0,
          "TOTAL": 0
        },
        "ibmxforce": {
          "INFO": 0,
          "LOW": 0,
          "MEDIUM": 0,
          "CRITICAL": 0,
          "HIGH": 0,
          "TOTAL": 0
        },
        "alienvault": {
          "INFO": 0,
          "LOW": 0,
          "MEDIUM": 0,
          "CRITICAL": 0,
          "HIGH": 0,
          "TOTAL": 0
        }
      },
      "rules": [
        {
          "name": "Windows Defender Anti-Malware Alerts",
          "count": 6
        },
        {
          "name": "UAC Bypass via Event Viewer",
          "count": 1
        }
      ]
    }
  }
```

Get host distribution based on platform

Use this API to fetch platform-wise count for hosts (further categorized based on the host state).

URL

/hosts/count

Request type

GET

Example response format

```
{
  "status": "success",
  "message": "Successfully fetched the nodes status count",
  "data": {
    "windows": {
      "online": 0,
      "offline": 9
    },
    "linux": {
      "online": 0,
      "offline": 3
    },
    "darwin": {
      "online": 0,
      "offline": 1
    }
  }
}
```

Get additional configuration applied through tags

Use this API to fetch details of additional configuration, such as queries and packs applied to a host through tags.

URL

/hosts/additional_config

Request type

POST

Example payload format:

```
{
  "node_id": 13
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
host_identifier	Required if node_id is not specified	String	Specifies the identifier of the host.
node_id	Required if host_identifier is not specified	Integer	Specifies the node identifier of the host.

Example response format


```
{
  "status": "success",
  "message": "Successfully fetched additional config of the node for the
host identifier passed",
  "data": {
    "queries": [],
    "packs": [
      {
        "id": 13,
        "platform": null,
        "version": null,
        "shard": null,
        "discovery": [],
        "queries": {
          "win_file_events": {
            "id": 101,
            "name": "win_file_events",
            "query": "select * from processes;",
            "interval": 30,
            "platform": "windows",
            "version": "2.9.0",
            "description": "Processes",
            "value": "Processes",
            "removed": false,
            "shard": null,
            "snapshot": false,
            "tags": [],
            "packs": [
              "response 123"
            ]
          }
        },
        "name": "response 123",
        "tags": [
          "jane"
        ]
      }
    ],
    "tags": [
      "janetest"
    ]
```

```
  }
}
```

Get complete configuration applied to an agent

Use this API to fetch all configuration applied to a specific host.

URL

/hosts/config

Request type

POST

Example payload format:

```
{
  "node_id": 13
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
host_identifier	Required if node_id is not specified	String	Specifies the identifier of the host.
node_id	Required if host_identifier is not specified	Integer	Specifies the node identifier of the host.

Example response format:

```
{
  "status": "success",
  "message": "Successfully fetched full config of the node for the
host identifier passed",
  "data": {
    "options": {
      "custom_plgx_EnableLogging": "true",
      "enable_powershell_events_subscriber": "true"
    },
    "feature_vectors": {
      "character_frequencies": [
        0
      ]
    },
    "win_include_paths": {
      "all_files": [
        "*"
      ]
    },
    "plgx_event_filters": {
      "win_ssl_events": {
        "process_name": {
```

```
          "exclude": {
            "values": [
              "*\\Program Files\\plgx_osquery\\plgx_*"
            ]
          }
        }
      }
    },
    "schedule": {
      "appcompat_shims": {
        "id": 150,
        "query": "select ach.*,(select sha1 from win_hash wh where
wh.path=ach.path limit 1 ) as sha1 from appcompat_shims ach;",
        "interval": 3600,
        "platform": "windows",
        "version": null,
        "description": "Windows scheduled_tasks",
        "value": null,
        "removed": false,
        "shard": null,
        "snapshot": false,
        "status": true
      }
    },
    "packs": [
      {
        "id": 13,
        "platform": null,
        "version": null,
        "shard": null,
        "discovery": [],
        "queries": {
          "win_file_events": {
            "id": 101,
            "name": "win_file_events",
            "query": "select * from processes;",
            "interval": 30,
            "platform": "windows",
            "version": "2.9.0",
            "description": "Processes",
            "value": "Processes",
            "removed": false,
            "shard": null,
            "snapshot": false,
            "tags": [],
            "packs": [
              "response 123"
            ]
          }
        },
        "name": "response 123",
        "tags": [
```

```
            "ajay"
          ]
        }
      ]
    }
  }
```

Get event count for each applied query for a host

Use this API to fetch the event count for each query applied to a specific host.

URL

/hosts/recent_activity/count

Request type

POST

Example payload format

```
{
  "node_id": 13
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
host_identifier	Required if node_id is not specified	String	Specifies the identifier of the host.
node_id	Required if host_identifier is not specified	Integer	Specifies the node identifier of the host.

Example response format

```
{
  "status": "success",
  "message": "Successfully fetched the count of schedule query results
count of host identifier passed",
  "data": [
    {
      "name": "windows_real_time_events",
      "count": 6318
    }
  ]
}
```

Get events generated for a host based a query

Use this API to fetch events generated for a specific host based on a query. Results can be filtered by using pagination and search terms.

URL

/hosts/recent_activity

Request type

POST

Example payload format

```
{
  "start": 0,
  "limit": 10,
  "node_id": 13,
  "query_name": "windows_real_time_events",
  "searchterm": ""
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
host_identifier	Required if node_id is not specified	String	Specifies the identifier of the host.
node_id	Required if host_identifier is not specified	Integer	Specifies the node identifier of the host.
query_name	Required	String	Specifies the name of the query to filter the results.
column_name	Optional	String	Specifies the name of the column based on which to filter the event results. This is used in conjunction with column_value.
column_value	Optional	String	Represents the value to apply to the specified column. This is used in conjunction with column_name.
start	Optional	Integer	Specifies the start value of the results. This value is use for pagination. By default, this is set to 0.
limit	Optional	Integer	Specifies the end value of the results. This value is use for pagination. By default, this is set to 10.
searchterm	Optional	String	Specifies the term to filter the search results. Only results containing the searchterm are returned.

Example response format


```
{
  "status": "success",
  "message": "Successfully fetched the count of schedule query results
count of host identifier passed",
  "data": {
    "count": 6318,
    "total_count": 6318,
    "categorized_count": 6318,
    "results": [
      {
        "id": 199205,
        "timestamp": "02/03/2022 09/40/53",
        "action": "added",
        "columns": {
          "eid": "3CEF28D2-3CFF-4B18-87D6-5C3505CDFFFF",
          "time": "1643881236",
          "action": "REMOTE_THREAD_CREATE",
          "eventid": "3",
          "src_pid": "4",
          "src_path": "System",
          "utc_time": "Thu Feb  3 09:40:36 2022",
          "owner_uid": "JANE\\jane doe",
          "target_pid": "1412",
          "module_name": "ntdll.dll",
          "target_path": "C:\\Windows\\System32\\conhost.exe",
          "src_process_guid": "1665D422-84B8-11EC-82B8-0209D9237A0A",
          "target_process_guid": "1665D568-84B8-11EC-82B8-0209D9237A0A"
        }
      }
    ]
  }
}
```


Export events generated for a host based on a query

Use this API to export (to a CSV file) events generated for a host based on a specific query. You can use filters to narrow the list of exported events.

URL

/hosts/search/export

Request type

POST

Example payload format


```
{
  "node_id": 13,
  "query_name": "os_version"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
host_identifier	Required if node_id is not specified	String	Specifies the identifier of the host.
node_id	Required if host_identifier is not specified	Integer	Specifies the node identifier of the host.
query_name	Required	String	Specifies the name of the query to filter the results.
column_name	Optional	String	Specifies the name of the column based on which to filter the event results. This is used in conjunction with column_value.
column_value	Optional	String	Represents the value to apply to the specified column. This is used in conjunction with column_name.
conditions	Optional	JSON	Specifies one or more conditions (in JSON format) to narrow down the fetched results.

Get all the tags applied to a host

Use this API to fetch a list of all tags applied to a host.

URL

/hosts/<node_id>/tags

Request type

GET

Example response format

```
{
	"status": "success",
	"message": "Successfully fetched the tags of host",
	"data": [
		"ajtest"
	]
}
```

Assign a tag to a host

Use this API to apply a tag to a host.

URL

/hosts/<node_id>/tags

Request type

POST

Example payload format

```
{
  "tag": "foo"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
tag	Required	string	Specifies the tag to be assigned.

Example response format

```
{
  "status": "success",
  "message": "Successfully created tags to host"
}
```

Remove a tag from a host

Use this API to remove a tag from a host.

URL

/hosts/<node_id>/tags

Request type

DELETE

Example payload format

```
{
  "tag": "foo"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
tag	Required	string	Specifies the tag to be removed.

Example response format

```
{
  "status": "success",
  "message": "Successfully removed tags from host"
}
```

Deactivate a host

Use this API to no longer monitor activity for a host or receive data from the host.

Note: If needed, a deactivated host can be reverted to active status.

URL

/hosts/<node_id>/delete

Request type

PUT

Example response format

```
{
  "status": "Success",
  "message": "Successfully removed the host"
}
```

Reactivate a removed host

Use this API to reactivate a host after it is removed.

URL

/hosts/<node_id>/enable

Request type

PUT

Example response format

```
{
  "status": "Success",
  "message": "Successfully enabled the host"
}
```

Enable hosts

Use this API to enable one or more managed hosts. You can enable an archived host and move it back to Active status.

URL

/hosts/enable

Request type

POST

Example response format

```
    {
            "host_identifiers": "Foo,Foobar"
    }
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
host_identifiers	Required if node_ids is not specified	String	Specifies the host IDs. When specifying multiple values, separate each value using a comma.
node_ids	Required if host_identifiers is not specified	String	Specifies the node IDs. When specifying multiple values, separate each value using a comma.

Example response format

```
{
        "status": "success",
        "message": "Successfully enabled the host"
}
```

Delete hosts

Use this API to permanently delete one or more hosts.

URL

/hosts/delete

Request type

DELETE

Example response format

```
{
        "host_identifiers": "Foo,Foobar"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
host_identifiers	Required if node_ids is not specified	String	Specifies the host IDs. When specifying multiple values, separate each value using a comma.
node_ids	Required if host_identifiers is not specified	String	Specifies the node IDs. When specifying multiple values, separate each value using a comma.

Example response format

```
{
```

```
        "status": "success",
        "message": "Successfully deleted the host"
}
```

Archive hosts

Use this API to archive hosts. Archived hosts are displayed on the Hosts > Archived page and removed from the Hosts > Active page. No newer data is accepted from an archived endpoint.

Note: Archived hosts can be reverted and returned to Active status.

URL

/hosts/delete

Request type

PUT

Example response format

```
{
        "host_identifiers": "Foo,Foobar"
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
host_identifiers	Required if node_ids is not specified	String	Specifies the host IDs. When specifying multiple values, separate each value using a comma.
node_ids	Required if host_identifiers is not specified	String	Specifies the node IDs. When specifying multiple values, separate each value using a comma.

Example response format

```
{
     "status": "success",
     "message": "Successfully removed the host"
}
```

Delete a host

Use this API to permanently delete a host.

Note: Deleted hosts cannot be reverted. However, if you do not uninstall the EclecticIQ Endpoint Response client from the host before you delete the host, the host may be reactivated and monitored by the server if the host reconnects to the server.

URL

/hosts/<node_id>/delete

Request type

DELETE

Example response format

```
{
  "status": "Success",
  "message": "Successfully deleted the host"
}
```

Get status logs for a host

Use this API to fetch osquery agent logs for a host.

URL

/hosts/status_logs

Request type

POST

Example payload format

```
{
  "start": 0,
  "limit": 10,
  "node_id": 13
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
host_identifier	Required if node_id is not specified	String	Specifies the identifier of the host.
node_id	Required if host_identifier is not specified	Integer	Specifies the node identifier of the host.
start	Optional	integer	Specifies the start value of the results. This value is use for pagination. By default, this is set to 0.
limit	Optional	integer	Specifies the end value of the results. This value is use for pagination. By default, this is set to 10.

searchterm	Optional	string	Specifies the term to filter the search results. Only results containing the searchterm are returned.

Example response format:

```
{
  "status": "success",
  "message": "Successfully fetched the host's status logs",
  "data": {
    "results": [
      {
        "line": 326,
        "message": "Scheduled query may have failed:
process_memory_open_sockets",
        "severity": 1,
        "filename": "config.cpp",
        "created": "2022-02-03T07:15:42.131364",
        "version": "4.7.0"
      }
    ],
    "count": 1,
    "total_count": 1
  }
}
```

Export status logs for a host

Use this API to export osquery logs for a host.

URL

/hosts/status_log/export

Request type

POST

Example payload format

```
{
  "node_id": 13
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
host_identifier	Required if node_id is not specified	String	Specifies the identifier of the host.
node_id	Required if host_identifier is not specified	Integer	Specifies the node identifier of the host.

searchterm	Optional	string	Specifies the term to filter the search results. Only results containing the searchterm are returned.

Example response format

```
{
  "status": "Success",
  "message": "Downloading will be completed in sometime"
}
```

Alerts

This section describes APIs that help in alert management.

Get alert distribution based on source

Use this API to retrieve alert distribution based on source, such as source, such as IOC, rules, VirusTotal, IBMxForce, and AlienVault. You can also view the alert count for each source. You can use filters and fetch details for all hosts and rules, specific hosts, or specific rules.

URL

/alerts/count_by_source

Request type

GET

Example payload format

```
{
  "duration": "3",
  "date": "2022-2-7"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
resolved	Optional	Boolean	Specifies whether to fetch only resolved alerts. Possible values are true and false. • true fetches only resolved alerts • false fetches only non-resolved alerts
host_identifier	Optional	String	Specifies the identifier of a host to fetch alerts only for the specified host.
rule_id	Optional	Integer	Specifies the identifier for a rule to filter and fetch alerts for the specified rule.

duration	Optional	Integer	Specifies the duration input for the type parameter. Possible values are: • 1 for hour • 2 for day • 3 for week • 4 for month By default, this is set to 3.
type	Optional	Integer	Indicates the type of the timestamp to use. You can use either started_by or ending_by options. Possible values are: • 1 to filter the results based on starting (filters the events till the timestamp given) • 2 to filter the results based on ending (filters results starting from the timestamp given) By default, this is set to 2.
date	Optional	String	Represents the date for filtering the results for the type parameter. The format is (YYYY-MM-DD).

Example response format

```
{
  "status": "success",
  "message": "Data is fetched successfully",
  "data": {
    "alert_source": [
      {
        "name": "rule",
        "count": 662
      }
    ]
  }
}
```

Get a list of all events that generated alerts

Use this API to fetch a list of all events that generated alerts on the EclecticIQ Endpoint Response server. The event list includes details, such as time and source. On the EclecticIQ Endpoint Response server, this data is used to plot a timeline graph on Alerts page.

This API is available only in the Enterprise Edition of EclecticIQ Endpoint Response and unavailable in the Community Edition.

URL

/alerts/graph

Request type

GET

Example payload format

```
{
  "source": "rule",
  "duration": "3",
  "host_identifier": "Foobar",
  "rule_id ": 1,
  "date": "2022-2-7"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
host_identifier	Optional	String	Indicates host IDs to filter the fetched alerts. If a value is specified, only alerts generated for the provided node are returned.
rule_id	Optional	String	Indicates rule IDs to filter the fetched alerts. If a value is specified, only alerts generated for the provided rule id are returned. When specifying multiple values, separate each value using a comma.
source	Optional	String	Specifies the source of the alert. Possible values are: • rule • ioc • virustotal • alienvault
duration	Optional	Integer	Specifies the duration input for the type parameter. Possible values are: • 1 for hour • 2 for day • 3 for week • 4 for month By default, this is set to 3.
type	Optional	Integer	Indicates the type of the timestamp to use. You can use either started_by or ending_by options. Possible values are: • 1 to filter the results based on starting (filters the events till the timestamp given)

			• 2 to filter the results based on ending (filters results starting from the timestamp given) By default, this is set to 2.
date	Optional	String	Represents the date for filtering the results for the type parameter. The format is (YYYY-MM-DD).
severity	Optional	String	Specifies the severity for the alert. Possible values are High, Medium, Low, Info, and Critical.
verdict	Optional	String	Specifies the verdict added when resolving or opening an alert. Possible values are true_positive, false_positive, and open.
start_date	Optional	String	Specifies the start date to fetch alerts.
end_date	Optional	String	Specifies the end date to fetch alerts.
search	Optional	String	Specifies the term to filter the search results. Only results containing the specified term are returned.

Example response format

```
{
  "status": "success",
  "message": "Data is fetched successfully",
  "data": [
    {
      "start": 1643388024096.873,
      "content": "",
      "event_id": 1017,
      "className": ""
    }
  ]
}
```

Get a list of all alerts

Use the API to fetch the list of all alerts. This list can be filtered based on host, rule ID, query, and source.

URL

/alerts

Request type

POST

Example payload format

```
{
  "start": 0,
  "limit": 10,
  "source": "rule",
  "duration": "4",
  "searchterm": "",
  "date": "2022-1-28"
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
resolved	Optional	Boolean	Indicates whether to fetch resolved or unresolved alerts. Possible values are true and false. • true fetches only resolved alerts • false fetches only unresolved alerts By default, this is set to false.
events_count	Optional	Boolean	Specifies whether to fetch aggregated event counts. Possible values are true and false. • true fetches aggregated event counts • false ignores aggregated event count
host_identifier	Optional	String	Indicates host IDs to filter the fetched alerts. If a value is specified, only alerts generated for the provided node are returned.
rule_id	Optional	String	Indicates rule IDs to filter the fetched alerts. If a value is specified, only alerts generated for the provided rule id are returned. When specifying multiple values, separate each value using a comma.
source	Optional	String	Specifies the source of the alert. Possible values are: • rule • ioc • virustotal

			• alienvault
event_ids	Optional	Array of integers	Indicates event IDs to filter the fetched alerts. If a value is specified, only alerts generated for the provided event id are returned.
query_name	Optional	String	Specifies the name of the query to filter the alerts.
start	Optional	Integer	Specifies the start value of the results. This value is use for pagination. By default, this is set to 0.
limit	Optional	Integer	Specifies the end value of the results. This value is use for pagination. By default, this is set to 10.
searchterm	Optional	String	Specifies the term to filter the search results. Only results containing the *searchterm* are returned.
duration	Optional	Integer	Specifies the duration input for the type parameter. Possible values are: • 1 for hour • 2 for day • 3 for week • 4 for month By default, this is set to 3.
type	Optional	Integer	Indicates the type of the timestamp to use. You can use either started_by or ending_by options. Possible values are: • 1 to filter the results based on starting (filters the events till the timestamp given) • 2 to filter the results based on ending (filters results starting from the timestamp given) By default, this is set to 2.
date	Optional	String	Represents the date for filtering the results for the type parameter. The format is (YYYY-MM-DD).
column	Optional	String	Specifies the name of the column based on which to sort the results. This is used in conjunction with order_by.

order_by	Optional	String	Specifies how to sort the results. This is used in conjunction with column. Possible values are asc (for ascending) and desc (for descending).
severity	Optional	String	Specifies the severity for the alert. Possible values are High, Medium, Low, Info, and Critical.
verdict	Optional	String	Specifies the verdict added when resolving or opening an alert. Possible values are true_positive, false_positive, and open.
start_date	Optional	String	Specifies the start date to fetch alerts.
end_date	Optional	String	Specifies the end date to fetch alerts.

Example response format


```
{
  "status": "success",
  "message": "Data is fetched successfully",
  "data": {
    "count": 662,
    "total_count": 926,
    "results": [
      {
        "id": 1017,
        "query_name": "windows_real_time_events",
        "rule_id": 148,
        "node_id": 2,
        "severity": "INFO",
        "type": "rule",
        "recon_queries": "null",
        "result_log_uid": "41311451-3224-4153-a623-23d895123008",
        "source": "rule",
        "status": "OPEN",
        "verdict": null,
        "comment": null,
        "created_at": "28-01-2022 16:40:24",
        "updated_at": "28-01-2022 16:40:24",
        "aggregated_events_count": 27,
        "alerted_entry": {
          "eid": "76104FC6-DA33-4C33-B067-4A2600000000",
          "pid": "41332",
          "path": "C:\\Windows\\System32\\svchost.exe",
          "time": "1643388057",
```

```
            "action": "PROC_TERMINATE",
            "cmdline": "C:\\WINDOWS\\system32\\svchost.exe -k netsvcs -p
    -s wuauserv",
            "eventid": "2",
            "utc_time": "Fri Jan 28 16:40:57 2022",
            "owner_uid": "JANE\\jane doe",
            "parent_pid": "864",
            "parent_path": "C:\\Windows\\System32\\services.exe",
            "process_guid": "37DCA846-8031-11EC-ABDD-D4D25274449B",
            "parent_process_guid": "3BB5A207-7F94-11EC-ABDD-
    D4D25274449B"
          },
          "hostname": "host_1",
          "rule": {
            "name": "test_rule1",
            "id": 148
          }
        }
      ]
    }
  }
```


Update alert status

Use this API to update the status for an alert. You can set the alert status to indicate if the alert is resolved or open.

URL

/alerts

Request type

PUT

Example payload format


```
{
  "resolve": true,
  "alert_ids": [1017],
  "verdict": true,
  "comment": "Foobar"
}
```


Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
resolve	Optional	Boolean	Specifies whether to resolve or open an alert. Possible values are true and false. • true resolves the alert • false opens a resolved alert By default, the value is set to true.

alert_ids	Required	Array of integers	Specifies which alert IDs for the alerts to resolve or open.
verdict	Optional	Boolean	Specifies the verdict to add when resolving or opening an alert. Possible values are true and false. • true indicates a true positive verdict • false indicates a false positive verdict
comment	Optional	String	Indicates the comment to be added while resolving or opening the alert.

Example response format


```
{
  "status": "success",
  "message": "Selected alerts status is changed successfully"
}
```


Get information for an alert

Use this API to get detailed information for a specific alert.

URL

/alerts/<alert_id>

Request type

GET

Example response format


```
{
  "status": "success",
  "message": "Successfully fetched the Alerts data",
  "data": {
    "query_name": "windows_real_time_events",
    "message": {
      "eid": "62BDACFE-7F8B-4590-B803-BE1B00000000",
      "pid": "43560",
      "path": "C:\\Users\\jane
reddy\\AppData\\Local\\Microsoft\\OneDrive\\22.002.0103.0004\\FileCoAu
th.exe",
      "time": "1643387869",
      "action": "PROC_CREATE",
      "cmdline": "\"C:\\Users\\jane
reddy\\AppData\\Local\\Microsoft\\OneDrive\\22.002.0103.0004\\FileCoAu
th.exe\" -Embedding",
      "eventid": "2",
      "utc_time": "Fri Jan 28 16:37:49 2022",
      "owner_uid": "JANE\\jane doe",
      "parent_pid": "600",
```

```
        "parent_path": "C:\\Windows\\System32\\svchost.exe",
        "process_guid": "37DCA919-8031-11EC-ABDD-D4D25274449B",
        "parent_process_guid": "3BB5A22D-7F94-11EC-ABDD-D4D25274449B"
      },
      "node_id": 2,
      "rule_id": 148,
      "severity": "INFO",
      "created_at": "2022-01-28 16:37:46.275613",
      "type": "rule",
      "source": "rule",
      "recon_queries": "null",
      "status": "OPEN",
      "source_data": {},
      "rule": {
        "name": "test_rule1",
        "id": 148
      },
      "hostname": "host_1",
      "platform": "windows"
    }
}
```


Get related events for an alert

Use this API to fetch events that were generated within a +-30 second interval of an alert.

This API is available only in the Enterprise Edition of EclecticIQ Endpoint Response and unavailable in the Community Edition.

URL

/alerts/<alert_id>/events

Request type

GET

Example response format


```
{
  "status": "success",
  "message": "Successfully fetched the Alert's events data",
  "data": {
    "schedule_query_data_list_obj": [
      {
        "name": "windows_real_time_events",
        "data": [
          {
            "eid": "62BDACFE-7F8B-4590-B803-BE1B00000000",
            "pid": "43560",
            "path": "C:\\Users\\jane
reddy\\AppData\\Local\\Microsoft\\OneDrive\\22.002.0103.0004\\FileCoAu
th.exe",
            "time": "1643387869",
```

```
                "action": "PROC_CREATE",
                "cmdline": "\"C:\\Users\\jane
    reddy\\AppData\\Local\\Microsoft\\OneDrive\\22.002.0103.0004\\FileCoAu
    th.exe\" -Embedding",
                "eventid": "2",
                "utc_time": "Fri Jan 28 16:37:49 2022",
                "owner_uid": "JANE\\jane doe",
                "parent_pid": "600",
                "parent_path": "C:\\Windows\\System32\\svchost.exe",
                "process_guid": "37DCA919-8031-11EC-ABDD-D4D25274449B",
                "parent_process_guid": "3BB5A22D-7F94-11EC-ABDD-
    D4D25274449B",
                "date": "Fri Jan 28 16:37:49 2022 UTC"
              }
            ]
          }
        ],
        "system_state_data_list": [
          "patches",
          "os_version"
        ]
      }
    }
```


Get host operating system state for an alert

Use this API to fetch information for a host for which an alert was generated. This API fetches host state information, including applied patches and running operating system.

This API is available only in the Enterprise Edition of EclecticIQ Endpoint Response and unavailable in the Community Edition.

URL

/alerts/<alert_id>/state

Request type

GET

Example response format


```
{
  "status": "success",
  "message": "Successfully fetched the Alerted host state",
  "data": [
    {
      "query_name": "patches",
      "count": 29
    }
  ]
}
```

Get all aggregated events for an alert

Use this API to fetch events that were generated (during the aggregation interval) for a specific alert.

URL

/alerts/<alert_id>/alerted_events

Request type

POST

Example payload format

```
{
  "query_name": "windows_real_time_events",
  "start": 0,
  "limit": 10,
  "searchterm": ""
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
query_name	Optional	String	Specifies the name of the query for which to fetch events.
column_name	Optional	String	Specifies the name of the column based on which to filter the event results. This is used in conjunction with column_value.
column_value	Optional	String	Represents the value to apply to the specified column. This is used in conjunction with column_name.
start	Optional	Integer	Specifies the start value of the results. This value is use for pagination. By default, this is set to 0.
limit	Optional	Integer	Specifies the end value of the results. This value is use for pagination. By default, this is set to 10.
searchterm	Optional	String	Specifies the term to filter the search results. Only results containing the searchterm are returned.

Example response format

When query_name has not been given	<pre>{
	"status": "success",
	"message": "Successfully fetched the Alerted host state",</pre>

	"data": [
	{
	"query_name": "patches",
	"count": 29
	}
	]
	}

When query_name has been given	{
	"status": "success",
	"message": "Successfully fetched the Alert's events data",
	"data": {
	"total_count": 54,
	"count": 54,
	"results": [
	{
	"id": 116533,
	"columns": {
	"eid": "29CC2EF6-7E37-43A1-A425-9D0EC4000000",
	"pid": "14924",
	"time": "1643387992",
	"action": "SOCKET_CONNECT",
	"family": "AF_NET",
	"eventid": "10",
	"protocol": "6",
	"utc_time": "Fri Jan 28 16:39:52 2022",
	"event_type": "SOCKET",
	"local_port": "51205",
	"remote_port": "443",
	"process_guid": "3BB5A1D2-7F94-11EC-ABDD-D4D25274449B",
	"process_name": "C:\\Program Files\\Google\\Chrome\\Application\\chrome.exe",
	"local_address": "192.168.1.101",
	"remote_address": "52.182.143.211"
	},
	"action": "added",
	"timestamp": "2022-01-28 16:40:18"
	}
	]
	}
	}

Export all aggregated events for an alert

Use this API to export (to a CSV file) all the events that were generated (during the aggregation interval) for a specific alert.

URL

/alerts/<alert_id>/alerted_events/export

Request type

GET

Example payload format

```
{
  "query_name": "windows_real_time_events",
  "start": 0,
  "limit": 10,
  "searchterm": ""
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
query_name	Required	String	Specifies the name of the query for which to fetch events.
column_name	Optional	String	Name of the column based on which to filter the event results. This is used in conjunction with column_value.
column_value	Optional	String	Value to apply to the specified column. This is used in conjunction with column_name.
searchterm	Optional	String	Specifies the term to filter the search results. Only results containing the searchterm are returned.

Export alerts for a source, host, rule, or query

Use this API to export (to a CSV file) alerts based on the alerting source, host, rule, or query. Alerts can be filtered by using different criteria.

URL

/alerts/alert_source/export

Request type

POST

Example payload format

```
{
  "source": "rule",
  "duration": "4",
  "searchterm": "",
  "date": "2022-1-28"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
host_identifier	Optional	String	Indicates host IDs to filter the fetched alerts. If a value is specified, only alerts generated for the provided node are returned.
rule_id	Optional	Integer	Indicates rule IDs to filter the fetched alerts. If a value is specified, only alerts generated for the provided rule id are returned.
source	Optional	String	Specifies the source of the alert. Possible values are: • rule • ioc • virustotal • alienvault
event_ids	Optional	Array of integers	Indicates event IDs to filter the fetched alerts. If a value is specified, only alerts generated for the provided event id are returned.
duration	Optional	Integer	Specifies the duration input for the type parameter. Possible values are: • 1 for hour • 2 for day • 3 for week • 4 for month By default, this is set to 3.
type	Optional	Integer	Indicates the type of the timestamp to use. You can use either started_by or ending_by options. Possible values are: • 1 to filter the results based on starting (filters the events till the timestamp given) • 2 to filter the results based on ending (filters results starting from the timestamp given) By default, this is set to 2.

date	Optional	String	Represents the date for filtering the results for the type parameter. The format is (YYYY-MM-DD).
severity	Optional	String	Specifies the severity for the alert. Possible values are High, Medium, Low, Info, and Critical.
verdict	Optional	String	Specifies the verdict added when resolving or opening an alert. Possible values are true_positive, false_positive, and open.
start_date	Optional	String	Specifies the start date to fetch alerts.
end_date	Optional	String	Specifies the end date to fetch alerts.
search	Optional	String	Specifies the term to filter the search results. Only results containing the specified term are returned.

Get events associated with a process

Use this API to fetch the event category along with the count for a specific process. This API is relevant only for nodes running the Windows operating system.

This API is available only in the Enterprise Edition of EclecticIQ Endpoint Response and unavailable in the Community Edition.

URL

/alerts/process

Request type

POST

Example payload format

```
{
  "process_guid": "3BB5A22D-7F94-11EC-ABDD-D4D25274449B",
  "alert_id": "1016",
  "node_id": 2
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
process_guid	Required	String	Specifies the GUID of the process for which the events were generated.
node_id	Required	Integer	Specifies the unique identifier for the host for which the events are generated.
alert_id	Optional	String	Specifies the unique identifier for the generated alert.

Example response format


```
{
  "status": "success",
  "message": "Data is fetched successfully",
  "data": {
    "name": "svchost.exe",
    "path": "C:\\Windows\\System32\\svchost.exe",
    "all_children": [
      {
        "action": "PROC_CREATE",
        "count": 907,
        "color": "blue",
        "node_type": "action",
        "children": [
          {
            "color": "red",
            "name": "child",
            "data": {
              "eid": "2BC3F516-C644-4970-A992-D84300000000",
              "pid": "5276",
              "path": "C:\\Windows\\System32\\backgroundTaskHost.exe",
              "time": "1643341436",
              "action": "PROC_CREATE",
              "cmdline":
"\"C:\\WINDOWS\\system32\\backgroundTaskHost.exe\" -
ServerName:CortanaUI.AppX3bn25b6f886wmg6twh46972vprk9tnbf.mca",
              "eventid": "2",
              "utc_time": "Fri Jan 28 03:43:56 2022",
              "owner_uid": "JANE\\jane doe",
              "parent_pid": "600",
              "parent_path": "C:\\Windows\\System32\\svchost.exe",
              "process_guid": "3BB5A2E6-7F94-11EC-ABDD-D4D25274449B",
              "parent_process_guid": "3BB5A22D-7F94-11EC-ABDD-
D4D25274449B"
            },
            "has_child": true
          }
        ],
        "last_time": "1643387869",
```

```
        "all_children": [
          {
            "color": "red",
            "name": "child",
            "data": {
              "eid": "2BC3F516-C644-4970-A992-D84300000000",
              "pid": "5276",
              "path": "C:\\Windows\\System32\\backgroundTaskHost.exe",
              "time": "1643341436",
              "action": "PROC_CREATE",
              "cmdline":
"\"C:\\WINDOWS\\system32\\backgroundTaskHost.exe\" -
ServerName:CortanaUI.AppX3bn25b6f886wmg6twh46972vprk9tnbf.mca",
              "eventid": "2",
              "utc_time": "Fri Jan 28 03:43:56 2022",
              "owner_uid": "JANE\\jane doe",
              "parent_pid": "600",
              "parent_path": "C:\\Windows\\System32\\svchost.exe",
              "process_guid": "3BB5A2E6-7F94-11EC-ABDD-D4D25274449B",
              "parent_process_guid": "3BB5A22D-7F94-11EC-ABDD-
D4D25274449B"
            },
            "has_child": true
          }
        ],
        "name": "PROC_CREATE",
        "fetched": true,
        "process_guid": "3BB5A22D-7F94-11EC-ABDD-D4D25274449B"
      }
    ],
    "node_type": "root",
    "data": {
      "process_guid": "3BB5A22D-7F94-11EC-ABDD-D4D25274449B",
      "path": "C:\\Windows\\System32\\svchost.exe"
    }
  }
}
```


Get child events for a process

Use this API to fetch events spawned by a specific process. This API is relevant only for nodes running the Windows operating system.

This API is available only in the Enterprise Edition of EclecticIQ Endpoint Response and unavailable in the Community Edition.

URL

/alerts/process/child

Request type

POST

Example payload format

```
{
  "process_guid": "3BB5A4CE-7F94-11EC-ABDD-D4D25274449B",
  "action": "PROC_TERMINATE",
  "node_id": 2
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
process_guid	Required	String	Specifies the GUID of the process for which the events were generated.
action	Required	String	Indicates the action that occurred, such as process creation or process termination.
node_id	Required	Integer	Specifies the unique identified for the host for which the events are generated.
last_time	Optional	Integer	Represents the UNIX time to filter and fetch events generated until the specified time.

Example response format

```
{
  "status": "success",
  "message": "Successfully get the data",
  "data": {
    "child_data": [
      {
        "color": "red",
        "name": "child",
        "data": {
          "eid": "2087D9C2-06AE-4AEB-A566-DD2800000000",
          "pid": "3272",
          "path": "C:\\Windows\\System32\\backgroundTaskHost.exe",
          "time": "1643342965",
          "action": "PROC_TERMINATE",
          "cmdline": "\"C:\\WINDOWS\\system32\\backgroundTaskHost.exe\" -
ServerName:ShellFeedsUI.AppXnj65k2d1a1rnztt2t2nng5ctmk3e76pn.mca",
          "eventid": "2",
          "utc_time": "Fri Jan 28 04:09:25 2022",
          "owner_uid": "JANE\\jane doe",
          "parent_pid": "600",
          "parent_path": "C:\\Windows\\System32\\svchost.exe",
          "process_guid": "3BB5A4CE-7F94-11EC-ABDD-D4D25274449B",
          "parent_process_guid": "3BB5A22D-7F94-11EC-ABDD-D4D25274449B"
        }
      }
    ],
    "last_time": "1643342965"
  }
```

```
}
```

Get all analyst notes for an alert

Use this API to fetch all analyst notes associated with a specific alert.

This API is available only in the Enterprise Edition of EclecticIQ Endpoint Response and unavailable in the Community Edition.

URL

/alerts/<alert_id>/analyst/notes

Request type

GET

Example response format

```
{
  "status": "success",
  "message": "Successfully fetched the Analyst Notes data with
respective given alert id",
  "data": [
    {
      "id": 1,
      "notes": "test\n",
      "created_at": "2022-02-07T06:38:17.227820",
      "updated_at": "2022-02-07T06:38:17.227831",
      "user_id": 1,
      "user": "admin"
    }
  ]
}
```

Create an analyst note for an alert

Use this API to create an analyst note for an alert. Analyst notes can summarize your understanding and are useful for reference purposes and alert investigation.

This API is available only in the Enterprise Edition of EclecticIQ Endpoint Response and unavailable in the Community Edition.

URL

/alerts/<alert_id>/analyst/notes

Request type

POST

Example payload format

```
{
  "notes": "test"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
notes	Required	String	Specifies the text for the user note.

Example response format

```
{
  "status": "success",
  "message": "Successfully added notes",
  "data": {
    "Analyst_note_id": 1
  }
}
```

Update an analyst note for an alert

Use this API to update an existing analyst note associated with a specific alert.

This API is available only in the Enterprise Edition of EclecticIQ Endpoint Response and unavailable in the Community Edition.

URL

/alerts/<alert_id>/analyst/notes

Request type

PUT

Example payload format

```
{
  "notes": "test1",
  "note_id": 1
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
notes	Required	String	Specifies the text for the user note.
note_id	Required	Integer	Provides a unique identifier for the note.

Example response format

```
{
  "status": "success",
  "message": "Successfully modified the notes",
  "data": {
    "Analyst_note_id": 1
  }
}
```

Delete an analyst note for an alert

Use this API to delete an analyst note.

This API is available only in the Enterprise Edition of EclecticIQ Endpoint Response and unavailable in the Community Edition.

URL

/alerts/<alert_id>/analyst/notes

Request type

DELETE

Example payload format

```
{
  "note_id": 1
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
note_id	Required	Integer	Provides a unique identifier for the note.

Example response format

```
{
  "status": "success",
  "message": "Successfully removed notes"
}
```

Carves

This section describes APIs that help in managing carve files.

Get a list of all carve files

Use this API to fetch all the carve files present on the EclecticIQ Endpoint Response server. You can filter the craves list by using different criteria.

URL

/carves

Request type

POST

Example payload format

```
{
  "start": 0,
```

```
    "limit": 10,
    "searchterm": ""
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
host_identifier	Optional	string	Specifies a unique identifier for the host.
start	Optional	Integer	Specifies the start value of the results. This value is use for pagination. By default, this is set to 0.
limit	Optional	Integer	Specifies the end value of the results. This value is use for pagination. By default, this is set to 10.
searchterm	Optional	String	Specifies the term to filter the search results. Only results containing the searchterm are returned.
column	Optional	String	Specifies the name of the column based on which to sort the results. This is used in conjunction with order_by. Possible values are hostname and created_at.
order_by	Optional	String	Specifies how to sort the results. This is used in conjunction with column. Possible values are asc (for ascending) and desc (for descending).

Example response format


```
{
  "status": "success",
  "message": "Successfully fetched the Carves data",
  "data": {
    "count": 6,
    "results": [
      {
        "id": 10,
        "node_id": 12,
        "session_id": "YH0PVGLHGH",
        "carve_guid": "5095cd62-3738-407e-bb63-d7845bea4419",
        "carve_size": 583652352,
        "block_size": 300000,
        "block_count": 1946,
        "archive": null,
        "status": "IN PROGRESS",
```

```
            "created_at": "2022-02-07T07:11:43.518651",
            "hostname": "host_1"
          }
        ],
        "total_count": 6
      }
    }
```


Download a carve file

Use this API to download a carve file (in .TAR or .TAR.ZZ format) present on the EclecticIQ Endpoint Response server.

URL

/carves/download/<session_id>

Request type

GET

Delete a carve file

Use this API to delete a carve file from the EclecticIQ Endpoint Response server.

URL

/carves/delete

Request type

POST

Example payload format


```
    {
      "session_id": "5095cd62"
    }
```


Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
session_id	Required	String	Specifies the session ID of the carve file to delete.

Example response format


```
    {
      "status": "success",
      "message": "Successfully deleted the Carve for the session id
    given!"
    }
```

Config

This section describes APIs that help in managing configuration settings.

Get a list of all configs

Use this API to fetch the default configurations defined on the EclecticIQ Endpoint Response server for all platforms.

URL

/configs

Request type

GET

Example response format


```
{
  "status": "success",
  "message": "Successfully fetched the config data",
  "data": {
    "linux": {
      "Default": {
        "queries": {
          "arp_cache": {
            "id": 1,
            "query": "select * from arp_cache;",
            "interval": 86400,
            "platform": "linux",
            "version": null,
            "description": "Address resolution cache, both static and
dynamic (from ARP, NDP).",
            "value": null,
            "removed": false,
            "shard": null,
            "snapshot": false,
            "status": true
          }
        },
        "filters": {
          "events": {
            "disable_subscribers": [
              "user_events"
            ]
          },
          "options": {
            "custom_plgx_LogLevel": "3",
            "schedule_splay_percent": 10
          },
          "file_paths": {
            "binaries": [
```

```
            "/usr/bin/%%"
          ],
          "configuration": [
            "/etc/passwd"
          ]
        },
        "exclude_paths": {
          "binaries": [
            "/usr/bin/plgx-agent.log"
          ]
        }
      },
      "is_default": true,
      "id": 1,
      "conditions": null,
      "description": "Default configuration of linux hosts"
    }
  },
  "65arwin": {
    "Default": {
      "queries": {
        "arp_cache": {
          "id": 52,
          "query": "select * from arp_cache;",
          "interval": 86400,
          "platform": "65arwin",
          "version": null,
          "description": "Address resolution cache, both static and
dynamic (from ARP, NDP).",
          "value": null,
          "removed": false,
          "shard": null,
          "snapshot": false,
          "status": true
        }
      },
      "filters": {
        "options": {
          "custom_plgx_LogLevel": "3"
        },
        "file_paths": {
          "binaries": [
            "/usr/bin/%%"
          ],
          "configuration": [
            "/etc/%%"
          ]
        }
      },
      "is_default": true,
      "id": 2,
      "conditions": null,
```

```
        "description": "Default configuration of 66arwin hosts"
      }
    },
    "windows": {
      "Default": {
        "queries": {
          "appcompat_shims": {
            "id": 106,
            "query": "select ach.*,(select sha1 from win_hash wh where
wh.path=ach.path limit 1 ) as sha1 from appcompat_shims ach;",
            "interval": 3600,
            "platform": "windows",
            "version": null,
            "description": "Windows scheduled_tasks",
            "value": null,
            "removed": false,
            "shard": null,
            "snapshot": false,
            "status": true
          }
        },
        "filters": {
          "options": {
            "custom_plgx_LogLevel": "3"
          },
          "win_include_paths": {
            "all_files": [
              "*"
            ]
          },
          "plgx_event_filters": {
            "win_ssl_events": {
              "process_name": {
                "exclude": {
                  "values": [
                    "*\\Program Files\\plgx_osquery\\plgx_*"
                  ]
                }
              }
            }
          }
        },
        "is_default": true,
        "id": 3,
        "conditions": null,
        "description": "Default configuration of windows hosts"
      },
      "Deep": {
        "queries": {
          "ie_extensions": {
            "id": 161,
```

```
            "query": "select iee.*,(select sha1 from win_hash wh where
wh.path=iee.path limit 1 ) as sha1  from ie_extensions iee;",
            "interval": 86400,
            "platform": "windows",
            "version": null,
            "description": "Extensions in the Internet Explorer",
            "value": null,
            "removed": false,
            "shard": null,
            "snapshot": false,
            "status": true
          }
        },
        "filters": {
          "options": {
            "custom_plgx_LogLevel": "3"
          },
          "feature_vectors": {
            "character_frequencies": [
              0
            ]
          },
          "win_include_paths": {
            "all_files": [
              "*"
            ]
          },
          "plgx_event_filters": {
            "win_ssl_events": {
              "process_name": {
                "exclude": {
                  "values": [
                    "*\\Program Files\\plgx_osquery\\plgx_*"
                  ]
                }
              }
            }
          }
        },
        "is_default": false,
        "id": 4,
        "conditions": null,
        "description": "A Sample configuration with suggested queries
and filters to monitor host state"
      }
    }
  }
}
```

Add a config

Use this API to add a custom configuration for a platform.

URL

/configs

Request type

POST

Example payload format

```
{
  "conditions": {
    "hostname": {
      "value": "hha"
    },
    "os_name": {
      "value": "as"
    }
  },
  "queries": {
    "appcompat_shims": {
      "id": 106,
      "query": "select ach.*,(select sha1 from win_hash wh where
wh.path=ach.path limit 1 ) as sha1 from appcompat_shims ach;",
      "interval": 3600,
      "platform": "windows",
      "version": null,
      "description": "Windows scheduled_tasks",
      "value": null,
      "removed": false,
      "shard": null,
      "snapshot": false,
      "status": true
    }
  },
  "filters": {
    "options": {
      "custom_plgx_LogLevel": "3"
    }
  },
  "name": "test",
  "platform": "windows",
  "description": "test"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
conditions	Required	JSON	Specifies a list (in JSON format) of conditions (on host name and operating system) based on

			which the config is assigned. Hosts matching the conditions are assigned the config. If not specifying any conditions for the request, provide a blank JSON {}.
name	Required	String	Specifies the name for the config.
queries	Required	JSON	Specifies an array of queries (in JSON format) to include in the config. Here is the format to use when specifying queries. `{'query_name1': {'status':true, 'interval':100}, 'query_name2': {'status':false, 'interval':101}}`
filters	Optional	JSON	List (in JSON format) of filters specifying what to monitor and what not to monitor.
platform	Required	string	Specifies the type of hosts (based on the operating system) for which to use the config. Possible values are windows, linux, and darwin.
description	Optional	string	Provides a description for the config.

Example response format

```
{
  "status": "success",
  "message": "Config is added successfully",
  "data": 8
}
```

Get a config

Use this API to fetch a specific configuration for a platform based on its ID.

URL

/configs/<config_id>

Request type

GET

Example response format

```
{
  "status": "success",
  "message": "Fetched the config successfully",
  "data": {
    "queries": {
      "arp_cache": {
        "status": true,
```

```
        "interval": 86400
      }
    },
    "filters": {
      "options": {
        "custom_plgx_LogLevel": "3"
      }
    },
    "name": "Default",
    "description": "Default configuration of linux hosts",
    "conditions": null
  }
}
```

Update a config

Use this API to update an existing configuration defined for a platform.

URL

/configs/<config_id>

Request type

PUT

Example payload format

```
{
  "platform": "windows",
  "queries": {
    "appcompat_shims": {
      "id": 106,
      "query": "select ach.*,(select sha1 from win_hash wh where
wh.path=ach.path limit 1 ) as sha1 from appcompat_shims ach;",
      "interval": 3600,
      "platform": "windows",
      "version": null,
      "description": "Windows scheduled_tasks",
      "value": null,
      "removed": false,
      "shard": null,
      "snapshot": false,
      "status": true
    }
  },
  "filters": {
    "options": {
      "custom_plgx_LogLevel": "3"
    }
  },
  "conditions": {},
  "description": "Default configuration of windows hosts"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
conditions	Required	JSON (DICT)	Specifies a list (in JSON format) of conditions (on host name and operating system) based on which the config is assigned. Hosts matching the conditions are assigned the config. If not specifying any conditions for the request, provide a blank JSON {}.
filters	Optional	JSON	List (in JSON format) of filters specifying what to monitor and what not to monitor.
queries	Optional	JSON	Species an array of queries (in JSON format) to include in the config. Here is the format to use when specifying queries. `{'query_name1': {'status':true, 'interval':100}, 'query_name2': {'status':false, 'interval':101}}`
name	Optional	String	Provides a name for the config.
description	Optional	String	Provides a description for the config.

Example response format

```
{
  "status": "success",
  "message": "Config is updated successfully for the platform given"
}
```

Delete a config

Use this API to delete a specific configuration defined for a platform.

URL

/configs/<config_id>

Request type

DELETE

Example response format

```
{
  "status": "success",
  "message": "Config is deleted successfully"
}
```

Assign a config to hosts

Use this API to assign a configuration to one or more hosts based on host IDs or tags.

URL

/configs/<config_id>/assign

Request type

PUT

Example payload format

```
{
  "host_identifiers": "",
  "tags": "test,test1"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
host_identifiers	Required if tags are not specified	String	Specifies a list of host identifiers (comma separated).
tags	Required if host_identifiers is not specified	String	Specifies a list of tags (comma separated). All hosts with the specified tags are assigned the config.

Example response format

```
{
  "status": "success",
  "message": "Config is assigned to the hosts successfully"
}
```

Get a list of hosts assigned a config

Use this API to fetch the list of all hosts assigned a specific configuration.

URL

/configs/<config_id>/hosts

Request type

GET

Example response format

```
{
  "status": "success",
  "message": "Hosts are retried for the config",
  "data": [
    {
      "id": 3,
      "display_name": "C02XTC0MJG5J",
```

```
        "host_identifier": "2252194F-B7C8-5B64-9E6F-A4C197F6F97F",
        "os_info": {
          "arch": "x86_64",
          "name": "Mac OS X",
          "build": "19H15",
          "major": "10",
          "minor": "15",
          "patch": "7",
          "version": "10.15.7",
          "codename": "",
          "platform": "darwin",
          "platform_like": "darwin"
        },
        "tags": [],
        "last_ip": "136.185.178.140",
        "is_active": false
      }
    ]
}
```


Email

This section describes APIs that help in managing email settings.

Test mail credentials

Use this API to check the defined mail configuration by sending a test mail to the recipients.

URL

/email/test

Request type

POST

Example payload format


```
{
  "emailRecipients": "foobar@example.com",
  "email": "foo@example.com",
  "smtpAddress": "smtp.example.com",
  "password": "Foobar@123#",
  "smtpPort": "465",
  "use_ssl": true,
  "use_tls": false
}
```


Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
email	Required	String	Specifies the email ID from which to send the email.

smtpPort	Required	String	Specifies the port using which the SMTP server is authenticated.
smtpAddress	Required	String	Specifies the address using which the SMTP server is authenticated.
password	Required	String	Specifies the password using which to authenticate the SMTP server.
emailRecipients	Required	String	Provides the list of recipients (comma separated) to receive the test and alert emails.
use_ssl	Optional	Boolean	Indicates whether to use an SSL connection to the SMTP server. Specify a value of true to use SSL. By default, this is set to false.
use_tls	Optional	Boolean	Indicates whether to use an TLS connection to the SMTP server. Specify a value of true to use TLS. By default, this is set to false.

Example response format

```
{
  "status": "success",
  "message": "Successfully sent the email to recipients for the
existing configuration!"
}
```

Get mail configuration

Use this API to fetch the mail configuration currently being used for alerting through email.

URL

/email/configure

Request type

GET

Example response format

```
{
  "status": "success",
  "message": "Successfully fetched the email configuration",
  "data": {
    "emailRecipients": "foobar@example.com",
    "email": "foo@example.com",
    "smtpAddress": "smtp.example.com",
    "password": "Foobar@123#",
```

```
    "smtpPort": "465",
    "use_ssl": true,
    "use_tls": false
  }
}
```

Update mail configuration

Use this API to update the email configuration currently being used for alerting through email.

URL

/email/configure

Request type

POST

Example payload format

```
{
  "emailRecipients": "foobar@example.com",
  "email": "foo@example.com",
  "smtpAddress": "smtp.example.com",
  "password": "Foobar@123#",
  "smtpPort": "465",
  "use_ssl": true,
  "use_tls": false
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
email	Required	String	Specifies the email ID from which to send the email.
smtpPort	Required	String	Specifies the port using which the SMTP server is authenticated.
smtpAddress	Required	String	Specifies the address using which the SMTP server is authenticated.
password	Required	String	Specifies the password using which to authenticate the SMTP server.
emailRecipients	Required	String	Provides the list of recipients (comma separated) to receive the test and alert emails.
use_ssl	Optional	Boolean	Indicates whether to use an SSL connection to the SMTP server. Specify a value of true to use SSL.

			By default, this is set to false.
use_tls	Optional	Boolean	Indicates whether to use an TLS connection to the SMTP server. Specify a value of true to use TLS. By default, this is set to false.

Example response format

```
{
  "status": "success",
  "message": "Successfully updated the email settings!",
  "data": {
    "emailRecipients": "foobar@example.com",
    "email": "foo@example.com",
    "smtpAddress": "smtp.example.com",
    "password": "Foobar@123#",
    "smtpPort": "465",
    "use_ssl": true,
    "use_tls": false
  }
}
```

IOCs

This section describes APIs that help to manage existing IOCs (indicators of compromise).

Get a list of all indicators

Use this API to fetch all existing IOCs (indicators of compromise) from the EclecticIQ Endpoint Response server.

URL

/iocs

Request type

GET

Example response format

```
{
  "status": "success",
  "message": "Successfully fetched the IOCs",
  "data": {
    "test-intel_ipv4": {
      "type": "remote_address",
      "severity": "MEDIUM",
      "intel_type": "self",
      "values": "3.30.1.15,3.30.1.16"
```

```
        }
      }
    }
```

Update indicators

Use this API to update the existing IOCs (indicators of compromise) on the EclecticIQ Endpoint Response server.

URL

/iocs/add

Request type

POST

Example payload format

```
{
  "data": {
    "test-intel_ipv4": {
      "type": "remote_address",
      "severity": "MEDIUM",
      "intel_type": "self",
      "values": "3.30.1.15,3.30.1.16"
    }
  }
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
data	Required	JSON	Provides a list of IOCs (indicators of compromise) in JSON format. Here is an example. `{'data': {'test-intel_ipv4': {'type': 'remote_address','severity': 'MEDIUM','intel_type': 'self','values': '3.30.1.15,3.30.1.16'}}}"`

Example response format

```
{
  "status": "success",
  "message": "Successfully updated the intel data"
}
```

Management

This section describes APIs that help in managing server settings, such as email configuration, server options, Threat Intel keys, VirusTotal configuration, user passwords, log level values, log files, and server metrics.

Change password for a user

Use this API to change the login password for an existing EclecticIQ Endpoint Response user.

URL

/management/changepw

Request type

POST

Example payload format

```
{
  "old_password": "foobar@123#",
  "new_password": "Foobar@1234",
  "confirm_new_password": "Foobar@1234"
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
old_password	Required	String	Represents the old user password.
new_password	Required	String	Specifies the new user password.
confirm_new_password	Required	String	Specifies the new user password.

Example response format

```
{
  "status": "success",
  "message": "Password is updated successfully"
}
```

Verify password for a user

Use this API to verify the login password for an existing EclecticIQ Endpoint Response user.

URL

/management/verifypw

Request type

POST

Example payload format

```
{
  "password": "foobar@123#"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
password	Required	String	Specifies the user password to verify.

Example response format

```
{
  "status": "success",
  "message": "Password for the current user is verified successfully"
}
```

Update server configuration settings

Use this API to update EclecticIQ Endpoint Response server configuration settings, including SSO configuration, alert aggregation interval, and manual purge duration.

URL

/management/settings

Request type

PUT

Example payload format

```
{
  "purge_data_duration": "7",
  "alert_aggregation_duration": "60",
  "sso_enable": "true",
  "sso_configuration": {
    "idp_metadata_url": "https://idp.com",
    "app_name": "testt",
    "entity_id": "testid"
  }
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
purge_data_duration	Required	String	Specifies how long to retain the data. Data older than the specified number of days is deleted.
alert_aggregation_duration	Optional	String	Specifies the time window (in seconds) in which to aggregate events from the same host

			based on the same rule to an existing alert (rather than generating a new alert).
sso_enable	Optional	String	Specifies whether to enable SSO integration for the EclecticIQ Endpoint Response server. Possible values are true and false. By default, this is set to false.
sso_configuration	Optional	JSON	Specifies the settings to use for SSO configuration. Must include Entity ID, application name, and IDP URL.

Example response format

```
{
  "status": "success",
  "message": "Platform settings are updated successfully"
}
```

Get server configuration settings

Use this API to fetch EclecticIQ Endpoint Response server configuration settings, including SSO configuration, alert aggregation interval, and manual purge duration.

URL

/management/settings

Request type

GET

Example response format

```
{
  "status": "success",
  "message": "Platform settings are fetched successfully",
  "data": {
    "purge_data_duration": "7",
    "alert_aggregation_duration": "60",
    "sso_enable": "true",
    "sso_configuration": {
      "idp_metadata_url": "https://idp.com",
      "app_name": "testt",
      "entity_id": "testid"
    }
  }
}
```

Get Threat Intel API keys

Use this API to fetch the API keys configured to allow EclecticIQ Endpoint Response to work with threat intelligence sources.

URL

/management/apikeys

Request type

GET

Example response format

```
{
  "status": "success",
  "message": "Threat Intel keys are updated successfully",
  "data": {
    "virustotal": {
      "key":
"44c8b4325d9579f701cd4cc01c0c84c1c3887b67ca4eeb6cc2f923b24dbed31f"
    }
  }
}
```

Update Threat Intel API keys

Use this API to update the API keys configured to allow EclecticIQ Endpoint Response to work with threat intelligence sources.

URL

/management/apikeys

Request type

POST

Example payload format

```
{
  "IBMxForceKey": "",
  "IBMxForcePass": "",
  "vt_key":
"44c8b4325d9579f701cd4cc01c0c84c1c3887b67ca4eeb6cc2f923b24dbed31f",
  "otx_key": ""
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
vt_key	Optional	String	Represents the VirusTotal API key.
IBMxForceKey	Optional	String	Represents the IBMxForce key.
IBMxForcePass	Optional	String	Specifies the IBMxForce pass.
otx_key	Optional	String	Represents the AlienVault key.

Example response format


```
{
  "status": "success",
  "message": "Threat Intel keys are updated successfully",
  "data": {
    "virustotal": {
      "key":
"44c8b4325d9579f701cd4cc01c0c84c1c3887b67ca4eeb6cc2f923b24dbed31f"
    }
  }
}
```


Get VirusTotal engine configuration

Use this API to fetch the configuration settings for VirusTotal. The settings include the following values:

- AV engine – The VirusTotal database is a collection of multiple anti-virus (AV) engines. This value specifies the anti-virus engines with which to match file hashes. Even if one selected AV engine indicates that a file is harmful, an alert is generated.
  If any AV engine is set to false, the scanned result from that engine is ignored.
- Minimum Matching AV Count – This value comes into play if none of the selected AV engines provide a conclusive indication for a file hash. Then, the remainder of the AV engines are considered. This value specifies the number of non-selected AV engines that must indicate that a file is harmful before an alert is generated. An alert is generated only when the number of (non-selected) AV engines indicating indicating that the hash is unsafe is higher than the value specified for Minimum Matching AV Count.
- Retention period – Indicates the duration in days after which a file hash value is refreshed.

URL

/management/virustotal/av_engine

Request type

GET

Example response format


```
{
  "message": "virus total av engines are fetched successfully",
  "status": "success",
  "data": {
    "min_match_count": 3,
    "av_engines": {
      "Bkav": {
        "status": false
      }
    },
    "vt_scan_retention_period": 2
  }
}
```

Update VirusTotal engine configuration

Use this API to update the configuration settings for VirusTotal.

URL

/management/virustotal/av_engine

Request type

POST

Example payload format

```
{
  "min_match_count": 3,
  "av_engines": {
    "Bkav": {
      "status": false
    }
  },
  "vt_scan_retention_period": 2
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
min_match_count	Optional	Integer	If none of the selected AV engines provide a conclusive indication for a file hash, the other (non-selected) engines are considered. This value specifies the number of non-selected AV engines that must indicate that a file is harmful before an alert is generated. An alert is generated only when the number of (non-selected) AV engines indicating the file is harmful is higher than the specified value.
vt_scan_retention_period	Optional	Integer	Indicates the duration in days after which a file hash value is refreshed.
av_engines	Optional	JSON	Provides a list of specific AV engines to use for matching. Even if one selected AV engine indicates that a file is harmful, an alert is generated. If an AV engine is not selected, the scanned result from that engine is ignored.

Example response format

```
{
  "message": "VirusTotal AV engines configuration has been changed
successfully",
  "status": "success"
}
```

Get server log level setting

Use this API to fetch the current value for the log level setting for the EclecticIQ Endpoint Response server.

URL

/management/log_setting

Request type

GET

Example response format

```
{
  "message": "Log levels fetched",
  "status": "success",
  "data": {
    "log_level": "INFO"
  }
}
```

Update server log level setting

Use this API to update the log level for the EclecticIQ Endpoint Response server.

Here is the log level order:

- WARNING
- INFO
- DEBUG

The log level values are hierarchically inclusive. This implies that if you set the log level value to INFO, messages that have log levels above INFO (WARNING) are also included.

URL

/management/log_setting

Request type

PUT

Example payload format

```
{
  "er_log_level": "INFO",
  "er_ui_log_level": "INFO"
```

```
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
er_log_level	Optional	String	Specifies the log level to be set for the EclecticIQ Endpoint Response the plgx-esp_plgx-esp micro service. Possible values are WARNING, INFO, and DEBUG.
er_ui_log_level	Optional	String	Specifies the log level to be set for the EclecticIQ Endpoint Response plgx-esp_plgx-esp-ui micro service. Possible values are WARNING, INFO, and DEBUG.

Example response format

```
{
  "message": "Log level has been changed successfully",
  "status": "success"
}
```

Purge server data

Use this API to initiate an immediate background purge task. If the retention_days value is set, data for only the number of days specified is retained and all older data is deleted.

URL

/management/manual_purge

Request type

POST

Example payload format

```
{
  "rentention_days": 4
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
retention_days	Required	Integer	Specifies how long to retain the data. Data older than the specified number of days is deleted.

Example response format

```
{
```

```
  "message": "Manual purge triggered successfully",
  "status": "success"
}
```

Get a list of all log file names

Use this API to fetch names of all log files on the EclecticIQ Endpoint Response server. The fetched names can be passed to another API to download the files.

URL

/management/download_log

Request type

GET

Example response format

```
{
  "message": "Logs Downloaded successfully",
  "status": "success",
  "data": [
    "log"
  ]
}
```

Download a specific log file

Use this API to download a specific log file from the EclecticIQ Endpoint Response server based on the provided file name.

URL

/management/download_log

Request type

POST

Example payload format

```
{
  "server_name": "ER",
  "filename": "log"
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
server_name	Required	String	Specifies the name of the EclecticIQ Endpoint Response service from which to download the log file.

filename	Required	String	Specifies the name of log file name to download.

Example response format

Log files will be downloaded.

Fetch server metrics

Use this API to fetch EclecticIQ Endpoint Response server metrics, such as hourly client data volume, current requests awaiting processing and message statistics (for few micro services).

URL

/management/metrics

Request type

POST

Example payload format

```
{
  "from_time": "2022-02-07 11:00:00"
}
```

Payload parameters:

Parameter	*Parameter Type*	*Data type*	*Description*
from_time	Required	String	Specifies the time starting which to fetch server metrics data.

Example response format:

```
{
  "message": "Metrics fetched successfully",
  "status": "success",
  "data": {
    "TOPHOSTS": [],
    "DISKUSAGE": {
      "total": 48.41,
      "free": 28.86,
      "unit": "GB"
    },
    "NGINX": [],
    "POSTGRES": [
      {
        "created_at": "2022-02-07 13:58:51",
        "unit": "MB",
        "value": 791
      },
      {
        "created_at": "2022-02-07 12:58:51",
        "unit": "MB",
```

```
      "value": 791
    },
    {
      "created_at": "2022-02-07 11:58:51",
      "unit": "MB",
      "value": 791
    }
  ],
  "RABBITMQ": [
    {
      "created_at": "2022-02-07 13:58:51",
      "unit": null,
      "value": {
        "queue_totals": {
          "messages": 3,
          "messages_ready": 3,
          "messages_details": {
            "rate": 0.2
          },
          "messages_ready_details": {
            "rate": 0.2
          },
          "messages_unacknowledged": 0,
          "messages_unacknowledged_details": {
            "rate": 0
          }
        },
        "message_stats": {
          "ack": 228,
          "get": 0,
          "confirm": 0,
          "deliver": 228,
          "publish": 51323,
          "get_empty": 0,
          "redeliver": 0,
          "disk_reads": 0,
          "get_no_ack": 0,
          "ack_details": {
            "rate": 0
          },
          "deliver_get": 142951,
          "disk_writes": 228,
          "get_details": {
            "rate": 0
          },
          "deliver_no_ack": 142723,
          "confirm_details": {
            "rate": 0
          },
          "deliver_details": {
            "rate": 0
          },
```

```
        "drop_unroutable": 2,
        "publish_details": {
          "rate": 1.4
        },
        "get_empty_details": {
          "rate": 0
        },
        "redeliver_details": {
          "rate": 0
        },
        "return_unroutable": 0,
        "disk_reads_details": {
          "rate": 0
        },
        "get_no_ack_details": {
          "rate": 0
        },
        "deliver_get_details": {
          "rate": 2.8
        },
        "disk_writes_details": {
          "rate": 0
        },
        "deliver_no_ack_details": {
          "rate": 2.8
        },
        "drop_unroutable_details": {
          "rate": 0
        },
        "return_unroutable_details": {
          "rate": 0
        }
      },
      "object_totals": {
        "queues": 14,
        "channels": 29,
        "consumers": 12,
        "exchanges": 13,
        "connections": 25
      }
    }
  },
  {
    "created_at": "2022-02-07 12:58:51",
    "unit": null,
    "value": {
      "queue_totals": {
        "messages": 3,
        "messages_ready": 3,
        "messages_details": {
          "rate": 0
        },
```

```
    "messages_ready_details": {
      "rate": 0
    },
    "messages_unacknowledged": 0,
    "messages_unacknowledged_details": {
      "rate": 0
    }
  },
  "message_stats": {
    "ack": 212,
    "get": 0,
    "confirm": 0,
    "deliver": 212,
    "publish": 46926,
    "get_empty": 0,
    "redeliver": 0,
    "disk_reads": 0,
    "get_no_ack": 0,
    "ack_details": {
      "rate": 0
    },
    "deliver_get": 130658,
    "disk_writes": 212,
    "get_details": {
      "rate": 0
    },
    "deliver_no_ack": 130446,
    "confirm_details": {
      "rate": 0
    },
    "deliver_details": {
      "rate": 0
    },
    "drop_unroutable": 2,
    "publish_details": {
      "rate": 1
    },
    "get_empty_details": {
      "rate": 0
    },
    "redeliver_details": {
      "rate": 0
    },
    "return_unroutable": 0,
    "disk_reads_details": {
      "rate": 0
    },
    "get_no_ack_details": {
      "rate": 0
    },
    "deliver_get_details": {
      "rate": 4
```

```
      },
      "disk_writes_details": {
        "rate": 0
      },
      "deliver_no_ack_details": {
        "rate": 4
      },
      "drop_unroutable_details": {
        "rate": 0
      },
      "return_unroutable_details": {
        "rate": 0
      }
    },
    "object_totals": {
      "queues": 14,
      "channels": 29,
      "consumers": 12,
      "exchanges": 13,
      "connections": 25
    }
  }
},
{
  "created_at": "2022-02-07 11:58:51",
  "unit": null,
  "value": {
    "queue_totals": {
      "messages": 3,
      "messages_ready": 3,
      "messages_details": {
        "rate": 0
      },
      "messages_ready_details": {
        "rate": 0
      },
      "messages_unacknowledged": 0,
      "messages_unacknowledged_details": {
        "rate": 0
      }
    },
    "message_stats": {
      "ack": 196,
      "get": 0,
      "confirm": 0,
      "deliver": 196,
      "publish": 42530,
      "get_empty": 0,
      "redeliver": 0,
      "disk_reads": 0,
      "get_no_ack": 0,
      "ack_details": {
```

```
      "rate": 0
    },
    "deliver_get": 118374,
    "disk_writes": 196,
    "get_details": {
      "rate": 0
    },
    "deliver_no_ack": 118178,
    "confirm_details": {
      "rate": 0
    },
    "deliver_details": {
      "rate": 0
    },
    "drop_unroutable": 2,
    "publish_details": {
      "rate": 1.4
    },
    "get_empty_details": {
      "rate": 0
    },
    "redeliver_details": {
      "rate": 0
    },
    "return_unroutable": 0,
    "disk_reads_details": {
      "rate": 0
    },
    "get_no_ack_details": {
      "rate": 0
    },
    "deliver_get_details": {
      "rate": 2.8
    },
    "disk_writes_details": {
      "rate": 0
    },
    "deliver_no_ack_details": {
      "rate": 2.8
    },
    "drop_unroutable_details": {
      "rate": 0
    },
    "return_unroutable_details": {
      "rate": 0
    }
  },
  "object_totals": {
    "queues": 14,
    "channels": 29,
    "consumers": 12,
    "exchanges": 13,
```

```
                "connections": 25
              }
            }
          }
        ]
      }
    }
```

Packs

This section describes APIs that help in managing packs.

Get a list of all packs

Use this API to fetch a list of all packs defined on the EclecticIQ Endpoint Response server. You can filter the list of packs using different criteria.

URL

/packs

Request type

POST

Example payload format

```
{
  "start": 0,
  "limit": 25,
  "searchterm": ""
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
start	Optional	Integer	Specifies the start value of the results. This value is use for pagination. By default, this is set to 0.
limit	Optional	Integer	Specifies the end value of the results. This value is use for pagination. By default, this is set to 10.
searchterm	Optional	String	Specifies the term to filter the search results. Only results containing the searchterm are returned.

Example response format

```
{
```

```
  "status": "success",
  "message": "Successfully fetched the packs info",
  "data": {
    "count": 13,
    "total_count": 13,
    "results": [
      {
        "id": 1,
        "name": "all-events-pack",
        "platform": null,
        "version": null,
        "description": null,
        "shard": null,
        "category": "General",
        "tags": [],
        "queries": [
          {
            "id": 1,
            "name": "win_file_events",
            "sql": "select * from win_file_events;",
            "interval": 13,
            "platform": "windows",
            "version": "2.9.0",
            "description": "Windows File Events",
            "value": "File Events",
            "snapshot": false,
            "shard": null,
            "tags": [],
            "packs": [
              "all-events-pack"
            ]
          }
        ]
      }
    ]
  }
}
```


Get a pack

Use this API to fetch detailed information for a specific pack, including the tags associated with the pack.

URL

/packs/<pack_id>

Request type

GET

Example response format


```
{
```

```
  "status": "success",
  "message": "successfully fetched the packs info",
  "data": {
    "id": 1,
    "name": "all-events-pack",
    "platform": null,
    "version": null,
    "description": null,
    "shard": null,
    "category": "General",
    "tags": [],
    "queries": [
      "win_file_events"
    ]
  }
}
```


Add a pack using a JSON payload

Use this API to add a new pack to the EclecticIQ Endpoint Response server using a JSON payload.

URL

/packs/add

Request type

POST

Example payload format


```
{
  "tags": "test",
  "name": "test_pack",
  "queries": {
    "test_startup_items": {
      "query": "select * from startup_items;",
      "interval": 25,
      "platform": "windows",
      "version": "2.9.0",
      "description": "Executable File Events",
      "value": "Executable File Events",
      "snapshot": false,
      "shard": null,
      "tags": "test"
    }
  },
  "category": "General",
  "platform": "windows",
  "version": "1.0",
  "description": "Test pack",
  }
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
tags	Optional	String	Provides a list of one or more tags. When specifying multiple tags, separate each tag using a comma.
name	Required	String	Specifies the tag name.
queries	Required	JSON	Specifies a list of queries to be included in the pack.
category	Optional	String	Assigns a category to the pack. Possible values are: • Intrusion Detection • Monitoring • Compliance and Management • Forensics and Incident Response • General • Others
platform	Optional	String	Specifies a platform for the pack. Possible values are: • windows • linux • darwin
version	Optional	String	Specifies a version for the pack.
description	Optional	String	Provides a description for the pack.

Example response format

```
{
  "pack_id": 14,
  "message": "Imported query pack and pack is added/uploaded
successfully",
  "status": "success"
}
```

Add a pack using a file

Use this API to add a new pack by using a file. When using a file to create a pack, ensure that the file contents are is JSON format.

URL

/packs/upload

Request type

POST

Example payload format

```
{
  "file": <A File>,
  "category": "General"
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
file	Required	File	File containing the pack (in JSON format).
category	Optional	String	Assigns a category to the pack. Possible values are: • Intrusion Detection • Monitoring • Compliance and Management • Forensics and Incident Response • General • Others

Example response format

```
{
  "pack_id": 14,
  "message": "Imported query pack and pack is added/uploaded
successfully",
  "status": "success"
}
```

Get tags for a pack

Use this API to fetch all the tags associated with a specific pack.

URL

/packs/<pack_id>/tags

/packs/<pack_name>/tags

Request type

GET

Example response format

```
{
  "status": "success",
  "message": "Successfully fetched the tags of pack",
  "data": [
```

```
      "test"
    ]
}
```

Assign tags to a pack

Use this API to assign a tag to a specific pack.

URL

/packs/<pack_id>/tags

/packs/<pack_name>/tags

Request type

POST

Example payload format

```
{
  "tag": "finance"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
tag	Required	String	Specifies the tag to assign to the pack.

Example response format

```
{
  "status": "success",
  "message": "Successfully created the tag(s) to queries"
}
```

Remove a tag from a pack

Use this API to remove a tag associated with a specific pack.

URL

/packs/<pack_id>/tags

Request type

DELETE

Example payload format

```
{
  "tag": "finance"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*

tag	Required	String	Specifies the tag to remove for the pack.

Example response format

```
{
  "status": "success",
  "message": "Successfully removed tags from query"
}
```

Delete a pack

Use this API to permanently delete a pack from the EclecticIQ Endpoint Response server.

URL

/packs/<pack_id>/delete

/packs/<pack_name>/delete

Request type

DELETE

Example response format

```
{
  "message": "Successfully removed the pack",
  "status": "success"
}
```

Queries

This section describes APIs that help in managing queries.

Add a live or distributed query

Use this API to run a specific live query on one or more hosts.

URL

/distributed/add

Request type

POST

Example payload format

```
{
  "tags": "",
  "query": "select * from system_info;",
  "nodes": "EC21722A-E9F2-2F3A-17FD-14F025638289",
  "os_name": [
    "Ubuntu"
  ]
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
query	Required	String	Represents the SQL query to run against the agent.
tags	Required if nodes or os_name are not specified	String	Specifies one or more tags (comma separated) based on which to assign the query. The query is assigned to all hosts associated with the specified tags.
nodes	Required if tags or os_name are not specified	String	Specifies one or more (comma separated) host identifiers based on which to assign the query.
os_name	Required if tags or nodes are not specified	Array	Specifies the operating systems based on which to assign the query.
description	Optional	String	Provides a description for the query.

Example response format


```
{
  "status": "success",
  "message": "Distributed query has been sent successfully",
  "data": {
    "query_id": 1933,
    "onlineNodes": 2,
    "online_nodes_details": [
      {
        "host_identifier": "5326bf26-4672-c9f1-bdd9-c0185016d353",
        "hostname": "host1",
        "node_id": 12
      }
    ]
  }
}
```


Get query results

1. Make a connection from a web socket client to one of the following URLs.

```
wss://<server_IP>/esp-ui/distributed/result
wss://<server_IP>/esp-ui/websocket/distributed/result
```

2. Send the received query_id to the socket server.
3. Ensure the socket client listen to server till a message is received.
4. Close the web socket connection after receiving results.

Get a list of all queries

Use this API to fetch a list of all queries defined on the EclecticIQ Endpoint Response server. You can filter the list of queries by using different criteria.

URL

/queries

Request type

POST

Example payload format

```
{
  "start": 0,
  "limit": 1,
  "searchterm": "EC2"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
start	Optional	Integer	Specifies the start value of the results. This value is use for pagination. By default, this is set to 0.
limit	Optional	Integer	Specifies the end value of the results. This value is use for pagination. By default, this is set to 10.
searchterm	Optional	String	Specifies the term to filter the search results. Only results containing the searchterm are returned.

Example response format

```
{
  "status": "success",
  "message": "Successfully fetched the queries info!",
  "data": {
    "count": 103,
    "total_count": 103,
    "results": [
      {
        "id": 78,
        "name": "AppCompat",
        "sql": "select * from registry where
key='HKEY_LOCAL_MACHINE\\SOFTWARE\\%Microsoft\\Windows
NT\\CurrentVersion\\AppCompatFlags\\Layers'",
        "interval": 86400,
        "platform": null,
```

```
            "version": null,
            "description": "Check Applications opted in for DEP",
            "value": null,
            "snapshot": true,
            "shard": null,
            "tags": [],
            "packs": [
              "windows-hardening"
            ]
          }
        ]
      }
    }
```


Get a list of all queries contained in packs

Use this API to fetch a list of all queries that are included within packs on the EclecticIQ Endpoint Response server.

URL

/queries/packed

Request type

POST

Example payload format


```
    {
      "start": 0,
      "limit": 1,
      "searchterm": ""
    }
```


Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
start	Optional	Integer	Specifies the start value of the results. This value is use for pagination. By default, this is set to 0.
limit	Optional	Integer	Specifies the end value of the results. This value is use for pagination. By default, this is set to 10.
searchterm	Optional	String	Specifies the term to filter the search results. Only results containing the searchterm are returned.

Example response format


```
    {
      "status": "success",
```

```
  "message": "Successfully fetched the packed queries info",
  "data": {
    "count": 1,
    "total_count": 103,
    "results": [
      {
        "id": 78,
        "name": "AppCompat",
        "sql": "select * from registry where
key='HKEY_LOCAL_MACHINE\\SOFTWARE\\%Microsoft\\Windows
NT\\CurrentVersion\\AppCompatFlags\\Layers'",
        "interval": 86400,
        "platform": null,
        "version": null,
        "description": "Check Applications opted in for DEP",
        "value": null,
        "snapshot": true,
        "shard": null,
        "tags": [],
        "packs": [
          "windows-hardening"
        ]
      }
    ]
  }
}
```


Get a query

Use this API to fetch a specific query based on its ID.

URL

/queries/<query_id>

Request type

GET

Example response format


```
{
  "status": "success",
  "message": "Successfully fetched the query info for the given id",
  "data": {
    "id": 78,
    "name": "AppCompat",
    "sql": "select * from registry where
key='HKEY_LOCAL_MACHINE\\SOFTWARE\\%Microsoft\\Windows
NT\\CurrentVersion\\AppCompatFlags\\Layers'",
    "interval": 86400,
    "platform": null,
    "version": null,
    "description": "Check Applications opted in for DEP",
    "value": null,
```

```
      "snapshot": true,
      "shard": null,
      "tags": [],
      "packs": [
        "windows-hardening"
      ]
    }
}
```

Add a query

Use this API to add a new query. This API only adds the query to the EclecticIQ Endpoint Response server; the added query is not assigned to any hosts.

URL

/queries/add

Request type

POST

Example payload format

```
{
  "name": "running_process_query",
  "query": "select * from processes;",
  "interval": 5,
  "platform": "windows",
  "version": "2.9.0",
  "snapshot": "true",
  "description": "Processes",
  "value": "Processes",
  "tags": "finance,sales"
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
name	Required	String	Specifies the name of the query.
query	Required	String	Represents the SQL query to add.
interval	Required	Integer	Specifies how often (in seconds) to run the query.
tags	Optional	String	Specifies one or more tags (comma separated) to assign to the query.
platform	Optional	String	Specifies the platform for the query. By default, this is set to all. Possible values are:

			• all • windows • linux • darwin • freebsd • posix
version	Optional	String	Specifies the version for the query.
description	Optional	String	Provides a description for the query.
snapshot	Optional	String	Specifies whether to make the query a snapshot query. Possible values are true and false. By default, this is set to true.
packs	Optional	String	Specifies one or more (comma separated) packs to assign to the query.

Example response format

```
{
  "status": "success",
  "message": "Successfully added the query for the data given",
  "query_id": 2
}
```

Update a query

Use this API to update a specific query.

URL

/queries/<query_id>

Request type

POST

Example payload format

```
{
  "name": "running_process_query",
  "query": "select * from processes;",
  "interval": 5,
  "platform": "windows",
  "version": "2.9.0",
  "snapshot": "true",
  "description": "Processes",
  "value": "Processes",
  "tags": "finance,sales"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
name	Required	String	Specifies the name of the query to update.
query	Required	String	Represents the SQL query to update.
interval	Required	Integer	Specifies how often (in seconds) to run the query.
tags	Optional	String	Specifies one or more tags (comma separated) to assign to the query.
platform	Optional	String	Specifies the platform for the query. By default, this is set to all. Possible values are: • all • windows • linux • darwin • freebsd • posix
version	Optional	String	Specifies the version for the query.
description	Optional	String	Provides a description for the query.
snapshot	Optional	String	Specifies whether to make the query a snapshot query. Possible values are true and false. By default, this is set to true.
packs	Optional	String	Specifies one or more (comma separated) packs to assign to the query.

Example response format


```
{
  "status": "success",
  "message": "Successfully edited the query info for the given id",
  "data": {
    "id": 78,
    "name": "AppCompat",
    "sql": "select * from registry where
key='HKEY_LOCAL_MACHINE\\SOFTWARE\\%Microsoft\\Windows
NT\\CurrentVersion\\AppCompatFlags\\Layers'",
    "interval": 86400,
    "platform": "all",
    "version": null,
    "description": "Check Applications opted in for DEP",
    "value": null,
    "snapshot": true,
```

```
      "shard": null
    }
  }
```

Get all tags for a query

Use this API to fetch a list of all tags associated with a specific query.

URL

/queries/<query_id>/tags

Request type

GET

Example response format

```
{
  "status": "success",
  "message": "Successfully fetched the tags of query",
  "data": [
    "test"
  ]
}
```

Assign tags to a query

Use this API to assign one or more new tags to a specific query (based on its ID).

URL

/queries/<query_id>/tags

Request type

POST

Example payload format

```
{
  "tag": "finance"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
tag	Required	String	Specifies the tag to be assigned to the query. When assigning multiple tags, ensure the tags are separated by commas.

Example response format

```
{
  "status": "success",
  "message": "Successfully created the tag(s) to queries"
```

```
}
```

Remove a specific tag associated with a query

Use this API to remove a specific tag associated with a query.

URL

/queries/<query_id>/tags

Request type

DELETE

Example payload format

```
{
  "tag": "finance"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
tag	Required	String	Specifies the tag to be removed from the query.

Example response format

```
{
  "status": "success",
  "message": "Successfully removed tags from query"
}
```

Delete a query

Use this API to permanently delete a specific query from the EclecticIQ Endpoint Response server.

URL

/queries/<query_id>/delete

/queries/<query_name>/delete

Request type

DELETE

Example response format

```
{
  "status": "success",
  "message": "Successfully deleted the query"
}
```

Rules

This section describes APIs that help in managing rules.

Get rule information

Use this API to fetch specific information for all rules. The fetched information includes rule name, status, and rule ID.

URL

/rules

Request type

GET

Example response format

```
{
  "status": "success",
  "message": "Successfully fetched the rules info",
  "data": [
    {
      "name": "rule1",
      "id": 1,
      "status": "ACTIVE"
    },
    {
      "name": "rule2",
      "id": 2,
      "status": "INACTIVE"
    }
  ]
}
```

Get a list of all rules

Use this API to fetch a list of all the rules defined on the EclecticIQ Endpoint Response server.

URL

/rules

Request type

POST

Example payload format

```
{
  "start": 0,
  "limit": 1,
  "searchterm": "EC",
  "alerts_count": true
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***

start	Optional	Integer	Specifies the start value of the results. This value is use for pagination. By default, this is set to 0.
limit	Optional	Integer	Specifies the end value of the results. This value is use for pagination. By default, this is set to 10.
searchterm	Optional	String	Specifies the term to filter the search results. Only results containing the *searchterm* are returned.
alerts_count	Optional	Boolean	Indicates whether to fetch alert count data. Possible values are true and false. Specify a value of true to fetch alert count for each. By default, this is set to true.
status	Optional	String	Indicates whether to fetch active or inactive rules. Possible values are true and false. Specify a value of true to fetch active rules and false to fetch inactive rules.
column	Optional	String	Specifies the name of the column based on which to sort the results. This is used in conjunction with order_by. Possible values are created_at, name, and alert_count.
order_by	Optional	String	Specifies how to sort the results. This is used in conjunction with column. Possible values are asc (for ascending) and desc (for descending).

Example response format


```
{
  "status": "success",
  "message": "Successfully fetched the rules info",
  "data": {
    "count": 147,
    "total_count": 147,
    "results": [
      {
        "id": 147,
        "alerters": [
          "debug"
        ],
```

```
            "conditions": {
              "rules": [
                {
                  "id": "action",
                  "type": "string",
                  "field": "action",
                  "input": "text",
                  "value": "test",
                  "operator": "equal"
                }
              ],
              "valid": true,
              "condition": "AND"
            },
            "description": "testing",
            "name": "test123",
            "severity": "INFO",
            "status": "ACTIVE",
            "updated_at": "2020-06-30T07:46:00.265400",
            "type": "MITRE",
            "tactics": [
              "defense-evasion"
            ],
            "technique_id": "T1070",
            "alerts_count": 23
          }
        ]
      }
    }
```


Get a rule

Use this API to fetch information for a specific rule (based on its ID).

URL

/rules/<rule_id>

Request type

GET

Example response format


```
    {
      "status": "success",
      "message": "Successfully fetched the rules info",
      "data": {
        "id": 147,
        "alerters": [
          "debug"
        ],
        "conditions": {
          "rules": [
```

```
            {
              "id": "action",
              "type": "string",
              "field": "action",
              "input": "text",
              "value": "test",
              "operator": "equal"
            }
          ],
          "valid": true,
          "condition": "AND"
        },
        "description": "tesing",
        "name": "test123",
        "severity": "INFO",
        "status": "ACTIVE",
        "updated_at": "2020-06-30T07:46:00.265400",
        "type": "MITRE",
        "tactics": [
          "defense-evasion"
        ],
        "technique_id": "T1070"
      }
    }
```


Modify a rule

Use this API to modify a specific rule. You can specify the rule to modify based on its ID.

URL

/rules/<rule_id>

Request type

POST

Example payload format


```
    {
      "alerters": "debug,email",
      "conditions": {
        "rules": [
          {
            "id": "action",
            "type": "string",
            "field": "action",
            "input": "text",
            "value": "test",
            "operator": "equal"
          }
        ],
        "valid": true,
        "condition": "AND"
```

```
    },
    "description": "tesing",
    "name": "test123",
    "severity": "INFO",
    "status": "ACTIVE",
    "updated_at": "2020-06-30T07:46:00.265400",
    "type": "MITRE",
    "tactics": "defense-evasion",
    "technique_id": "T1070, T1005"
}
```


Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
alerters	Optional	String	Specifies how information is shared for alerts generated based on this rule. When specifying multiple values, separate each value using a comma. Possible values are email, rsyslog, and debug.
name	Required	String	Provides the name of the rule.
description	Optional	String	Provides a description for the rule.
conditions	Required	JSON	Specifies a list of conditions (in JSON format) to match against the events.
severity	Optional	String	Specifies the severity for the alert generated based on the defined rule. Possible values are high, medium, low, info, and critical.
status	Optional	String	Specifies the status of the rule. Possible values are ACTIVE or INACTIVE. When set to INACTIVE, the rule is not matched against incoming events.
type	Optional	String	Indicates the type of rule. Possible values are MITRE and DEFAULT.
tactics	Optional	String	Specifies the tactics used in the rule. When specifying multiple values, separate each value using a comma.
technique_id	Optional	String	Indicates the IDs for the techniques an attacker may use for which the rule is

			written. When specifying multiple values, separate each value using a comma.
platform	Optional	String	Specifies the platform for the rule. Possible values are windows, linux, darwin, and all. By default, this is set to all.
alert_description	Optional	Boolean	Specifies whether to include the rule description in the email sent after alert generation. Possible values are true and false. By default, this is set to false.

Example response format


```
{
  "status": "success",
  "message": "Successfully modified the rules info",
  "data": {
    "id": 147,
    "alerters": [
      "debug"
    ],
    "conditions": {
      "rules": [
        {
          "id": "action",
          "type": "string",
          "field": "action",
          "input": "text",
          "value": "test",
          "operator": "equal"
        }
      ],
      "valid": true,
      "condition": "AND"
    },
    "description": "tesing",
    "name": "test123",
    "severity": "INFO",
    "status": "ACTIVE",
    "updated_at": "2020-06-30T07:46:00.265400",
    "type": "MITRE",
    "tactics": [
      "defense-evasion"
    ],
    "technique_id": "T1070"
  }
}
```

Add a rule

Use this API to create a new rule using JSON data.

URL

/rules/add

Request type

POST

Example payload format

```
{
  "alerters": "debug,email",
  "conditions": {
    "rules": [
      {
        "id": "action",
        "type": "string",
        "field": "action",
        "input": "text",
        "value": "test",
        "operator": "equal"
      }
    ],
    "valid": true,
    "condition": "AND"
  },
  "description": "tesing",
  "name": "test123",
  "severity": "INFO",
  "status": "ACTIVE",
  "updated_at": "2020-06-30T07:46:00.265400",
  "type": "MITRE",
  "tactics": "defense-evasion",
  "technique_id": "T1070, T1005"
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
alerters	Optional	String	Specifies how information is shared for alerts generated based on this rule. When specifying multiple values, separate each value using a comma. Possible values are email, rsyslog, and debug.
name	Required	String	Provides the name of the rule.
description	Optional	String	Provides a description for the rule.

conditions	Required	JSON	Specifies a list of conditions (in JSON format) to match against the events.
severity	Optional	String	Specifies the severity for the alert generated based on the defined rule Possible values are high, medium, low, info, and critical.
status	Optional	String	Specifies the status of the rule. Possible values are ACTIVE or INACTIVE. When set to INACTIVE, the rule is not matched against incoming events.
type	Optional	String	Indicates the type of rule. Possible values are MITRE and DEFAULT.
tactics	Optional	String	Specifies the tactics used in the rule. When specifying multiple values, separate each value using a comma.
technique_id	Optional	String	Indicates the IDs for the techniques an attacker may use for which the rule is written. When specifying multiple values, separate each value using a comma.
platform	Optional	String	Specifies the platform for the rule. Possible values are windows, linux, darwin, and all. By default, this is set to all.
alert_description	Optional	Boolean	Specifies whether to include the rule description in the email sent after alert generation. Possible values are true and false. By default, this is set to false.

Example response format

```
{
  "status": "success",
  "message": "Rule is added successfully ",
  "rule_id": 2
}
```

Activate rules

Use this API to activate or enable one or more rules based on the rule ID.

URL

/rules/enable

Request type

POST

Example payload format

```
{
  "rule_ids": [1, 2]
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
rule_ids	Required	Integer list	Specifies the list of rule identifiers for the rules to enable or activate.

Example response format

```
{
   "status": "success",
   "message": "Successfully modified the rules status"
}
```

Disable rules

Use this API to disable or deactivate one or more rules based on the rule IDs.

URL

/rules/disable

Request type

POST

Example payload format

```
{
  "rule_ids": [1, 2]
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
rule_ids	Required	Integer list	Specifies the list of rule IDs for the rules to disable or deactivate. When specifying multiple values, separate each value using a comma.

Example response format

```
{
```

```
    "status": "success",
    "message": "Successfully modified the rules status"
}
```

Delete rules

Use this API to permanently delete one or more rules based on the rule ID.

URL

/rules/disable

Request type

DELETE

Example payload format

```
{
  "rule_ids": [1, 2]
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
rule_ids	Required	Integer list	Specifies the list of rule identifiers for the rules to delete. When specifying multiple values, separate each value using a comma.

Example response format

```
{
"status": "success",
"message": "Successfully deleted the rule"
}
```

Get tactics for MITRE techniques

Use this API to fetch a list of tactics for the specified MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) techniques (based on their IDs). When specifying multiple technique IDs, separate the values with commas.

URL

/rules/tactics

Request type

POST

Example payload format

```
{
  "technique_ids": " T1005, T1004"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
technique_ids	Required	String	Indicates the IDs for the techniques for which list of tactics should be retrieved from MITRE site. When specifying multiple values, separate each value using a comma.

Example response format

```
{
  "status": "success",
  "message": "Tactics are fetched successfully from technique ids",
  "data": {
    "tactics": [
      "collection"
    ],
    "description": ""
  }
}
```

Schema

This section describes APIs that help in getting schema details.

Get schemas for all OSquery tables

Use this API fetch the complete schema for the agent.

URL

/schema

Request type

GET

Example payload format

```
{
  "export_type": "json"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
export_type	Optional	String	Specifies how to export the schema. Possible values are json or sql. Use json to get the schema in JSON format and sql to get the schema as SQL queries.

			By default, this is set to sql.

Example response format

SQL format

```
{
  "status": "success",
  "message": "Successfully fetched the schema",
  "data": {
    "account_policy_data": "CREATE TABLE
account_policy_data (uid BIGINT, creation_time DOUBLE,
failed_login_count BIGINT, failed_login_timestamp
DOUBLE, password_last_set_time DOUBLE)",
    "acpi_tables": "CREATE TABLE acpi_tables (name TEXT,
size INTEGER, md5 TEXT)"
  }
}
```

JSON

```
{
  "status": "success",
  "message": " EclecticIQ ESP agent schema is fetched
successfully",
  "data": [
    {
      "name": "etc_hosts",
      "description": "Line-parsed /etc/hosts.",
      "platform": [
        "windows",
        "linux",
        "darwin",
        "freebsd",
        "posix"
      ],
      "schema": {
        "address": {
          "type": "TEXT",
          "description": "IP address mapping",
          "is_required": false
        },
        "hostnames": {
          "type": "TEXT",
          "description": "Raw hosts mapping",
          "is_required": false
        }
      }
    }
  ]
}
```

Get schema for a OSQuery table

Use this API to fetch the table schema in SQL format for a specific OSQuery table from the agent.

URL

/schema/<table>

Request type

GET

Example response format

```
{
  "status": "success",
  "message": "Successfully fetched the table schema",
  "data": {
    "account_policy_data": "CREATE TABLE account_policy_data (uid
BIGINT, creation_time DOUBLE, failed_login_count BIGINT,
failed_login_timestamp DOUBLE, password_last_set_time DOUBLE)"
  }
}
```

Tags

This section describes APIs that help in managing tags.

Get a list of all tags

Use this API to fetch all the tags defined on the EclecticIQ Endpoint Response server.

URL

/tags

Request type

GET

Example payload format

```
{
  "searchterm": "test",
  "start": 0,
  "limit": 10
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
start	Optional	Integer	Specifies the start value of the results. This value is use for pagination. By default, this is set to 0.
limit	Optional	Integer	Specifies the end value of the results. This value is use for pagination.

			By default, this is set to 10.
searchterm	Optional	String	Specifies the term to filter the search results. Only results containing the searchterm are returned.
order_by	Optional	String	Specifies how to sort the results based on tag names. Possible values are asc (for ascending) and desc (for descending).

Example response format


```
{
  "status": "success",
  "message": "Successfully fetched the tags info",
  "data": {
    "count": 7,
    "total_count": 7,
    "results": [
      {
        "value": "test67",
        "nodes": [],
        "packs": [],
        "queries": [],
        "file_paths": []
      },
      {
        "value": "test",
        "nodes": [],
        "packs": [
          "all-events-pack"
        ],
        "queries": [
          "App_disabledExceptionChainValidation"
        ],
        "file_paths": []
      }
    ]
  }
}
```


Add a tag

Use this API to create a tag.

When a tag is created, it is available on the EclecticIQ Endpoint Response server but not assigned to any query, pack, or host.

URL

/tags/add

Request type

POST

Example payload format

```
{
  "tag": "test"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
tag	Required	String	Specifies the tag to add.

Example response format

```
{
  "status": "success",
  "message": "Tag is added successfully"
}
```

Delete tags

Use this API to permanently delete one or more tags from the EclecticIQ Endpoint Response server.

URL

/tags/delete

Request type

POST

Example payload format

```
{
  "tag": "test"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
tag	Required	String	Specifies the tags (comma separated values) to delete.

Example response format

```
{
  "status": "success",
  "message": "Tag is deleted successfully"
}
```

Get objects assigned a tag

Use this API to fetch all objects, such as hosts, queries, and packs associated with specific tags.

URL

/tags/tagged

Request type

POST

Example payload format

```
{
  "tags": "test"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
tags	Required	String	Specifies one or more tags (comma separated) for which to fetch associated objects.

Example response format

```
{
  "status": "success",
  "message": "All hosts, queries, packs for the tag provided!",
  "data": {
    "hosts": [
      {
        "id": 3,
        "display_name": "EC2AMAZ-2RJ1BIF",
        "host_identifier": "EC2CE2E2-3D74-1248-2FA9-23F2E960ED42",
        "os_info": {
          "name": "windows"
        },
        "tags": [
          "test"
        ],
        "last_ip": "15.206.168.222",
        "is_active": false
      }
    ],
    "packs": [
      {
        "id": 1,
        "name": "all-events-pack",
        "platform": null,
        "version": null,
        "description": null,
        "shard": null,
        "category": "General",
        "tags": [
          "test"
        ],
        "queries": [
          {
```

```
            "id": 2,
            "name": "win_process_events",
            "sql": "select * from win_process_events;",
            "interval": 38,
            "platform": "windows",
            "version": "2.9.0",
            "description": "Windows Process Events",
            "value": "Process Events",
            "snapshot": false,
            "shard": null,
            "tags": [],
            "packs": [
              "all-events-pack"
            ]
          }
        ]
      }
    ]
  }
}
```


Assign a tag to objects

Use this API to assign an existing tag to additional objects, such as hosts, queries, and packs.

URL

/tags/<tag_name>

Request type

PUT

Example payload format


```
{
"queries": [
       "win_process_events"
        "win_file_events"
  ]

"packs": [
     "windows-hardening"
  ]

"hosts": [
    "EC2300D6-B0D5-F9A6-1237-6553106EC525"
    "EC2100D9-B0D8-F2A3-1456-3454536EC222"
  ]

  "os_names": [
     "Windows 2012"
     "Windows 2016"
  ]
```

```
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
queries	Optional	Array	Specifies the queries to which to assign the tag.
packs	Optional	Array	Specifies the packs to which to assign the tag.
hosts	Optional	Array	Specifies the hosts to which to assign the tag.
os_names	Optional	Array	Specifies the operating systems to which to assign the tag. All hosts running the specified operating system are assigned the tag.

Example response format

```
{
"status""success",
"message":"Successfully assigned to the tag"

}
```

YARA

This section describes APIs that help in managing YARA files.

Get all YARA files

Use this API to fetch a list of all YARA files present on the EclecticIQ Endpoint Response server.

URL

/yara

Request type

GET

Example response format

```
{
  "status": "success",
  "message": "Successfully fetched the yara files",
  "data": {
    "windows": [
      "yarafileupload.yara",
      "yarafileupload2 - copy.yara",
      "darwinyara .yara",
      "untitled.yara",
      "eicar.yara"
    ],
    "linux": [
      "yarafileupload.yara",
```

```
        "yarafileupload2 - copy.yara",
        "yaratestfile - copy.yara",
        "eicar.yara",
        "log4jball.yara"
      ],
      "darwin": [
        "yarafileupload.yara",
        "eicar.yara"
      ]
    }
}
```

Upload a YARA file

Use this API to upload a YARA (.yara or .yar) file to the EclecticIQ Endpoint Response server.

URL

/yara/add

Request type

POST

Example payload format

```
{
  "file": <A YARA file>,
  "platform": "windows"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
file	Required	File	Provides the YARA file (.yar or .yara files only) containing the YARA rule.
platform	Required	String	Specifies the platform for the YARA file. Possible values are: • windows • linux • darwin

Example response format

```
{
  "status": "success",
  "message": "Successfully uploaded the file"
}
```

View YARA file content

Use this API to fetch the contents of a specific YARA file.

URL

/yara/view

Request type

POST

Example payload format

```
{
  "file_name": "eicar.yara"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
file_name	Required	String	Provides the name of the YARA file to view.

Example response format

```
{
  "status": "success",
  "message": "Successfully fetched the yara file content!",
  "data": "rule eicar_av_test {\n    /*\n       Per standard, match
only if entire file is EICAR string plus optional trailing
whitespace.\n       The raw EICAR string to be matched is:\n
X5O!P%@AP[4\\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-
FILE!$H+H*\n    */\n\n    meta:\n        description = \"This is a
standard AV test, intended to verify that BinaryAlert is working
correctly.\"\n        author = \"Jane Doe | ABC Corp\"\n
reference = \"http://www.eicar.org/86-0-Intended-use.html\"\n\n
strings:\n        $eicar_regex =
/^X5O!P%@AP\\[4\\\\PZX54\\(P\\^\\)7CC\\)7\\}\\$EICAR-STANDARD-
ANTIVIRUS-TEST-FILE!\\$H\\+H\\*\\s*$/\n\n    condition:\n        all
of them\n}\n\nrule eicar_substring_test {\n    /*\n       More generic
- match just the embedded EICAR string (e.g. in packed executables,
PDFs, etc)\n    */\n\n    meta:\n        description = \"Standard AV
test, checking for an EICAR substring\"\n        author = \"Jane Doe |
ABC Corp\"\n\n    strings:\n        $eicar_substring = \"$EICAR-
STANDARD-ANTIVIRUS-TEST-FILE!\"\n\n    condition:\n        all of
them\n}"
}
```

Update a YARA file

Use this API to update the associated platform for a specific YARA file on the EclecticIQ Endpoint Response server.

URL

/yara/update

Request type

PUT

Example payload format

```
{
  "file_name": "eicar.yara",
  "platform": "windows"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
file_name	Required	String	Provides the name of the YARA file to update.
platform	Required	String	Specifies the platform to associate with the specified YARA file. Possible values are: • windows • linux • darwin

Example response format:

```
{
  "status": "success",
  "message": "Successfully mapped to platform windows"
}
```

Delete a YARA file

Use this API to permanently delete a specific YARA file from the EclecticIQ Endpoint Response server.

URL

/yara/delete

Request type

POST

Example payload format

```
{
  "file_name": "eicar.yara",
  "platform": "windows"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*

file_name	Required	String	Provides the name of the YARA file to delete.
platform	Required	String	Specifies the platform for the YARA file to delete. Possible values are: • windows • linux • darwin

Example response format:

```
{
  "status": "success",
  "message": "File with the given file name is deleted successfully"
}
```

Hunt

This section describes APIs that help in managing hunts.

Hunt results by using a file (containing list of indicators)

Use this API to fetch data from multiple hosts by using a file containing a list of indicators. In an API call, you can hunt for only one type of indicator.

The API results are returned in JSON format. To export results to a CSV file, refer to the Export hunt results API.

URL

/hunt-upload

/indicators/upload

Request type

POST

Format 1

Example payload

```
{
  "file": <file of indicators>,
  "type": "md5"
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
file	Required	File	Provides a file containing a list of indicators. Each indicator in the file is separated by a new line.

type	Required	String	Indicates the type of hunt to perform. Possible values are: • md5 • sha256 • domain_name • ja3_md5 • process_guid • parent_process_guid • target_path • target_name • process_name • remote_address

Example response

```
{
  "status": "success",
  "message": "Successfully fetched the results through the hunt",
  "data": [
    {
      "hostname": "host_1",
      "host_identifier": "host_ID",
      "queries": [
        {
          "query_name": "osquery_info",
          "count": 1
        }
      ]
    }
  ]
}
```

Format 2

Example payload

```
{
  "file": <file of indicators>,
  "type": "md5",
  "host_identifier": "EC2300D6-B0D5-F9A6-1237-6553106EC525",
  "query_name": "win_file_events",
  "start": 2,
  "limit": 10
```

}

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***

file	Required for /hunt-upload and /indicators/upload	File	Provides a file containing a list of indicators. Each indicator in the file is separated by a new line.
type (for /hunt-upload) indicator_type (for /indicators/upload)	Required for both	String	Indicates the type of hunt to perform. Possible values are: • md5 • sha256 • domain_name • ja3_md5 • process_guid • parent_process_guid • target_path • target_name • process_name • remote_address
host_identifier	Required for /hunt-upload and /indicators/upload	String	Specifies the identifier of the host.
query_name	Required for /hunt-upload and /indicators/upload	String	Specifies the name of the query to filter the results.
start	Required for /hunt-upload and /indicators/upload	Integer	Specifies the start value of the results. This value is use for pagination. By default, this is set to 0.
limit	Required for /hunt-upload and /indicators/upload	Integer	Specifies the end value of the results. This value is use for pagination. By default, this is set to 10.
duration	Optional for /indicators/upload	Integer	Specifies the duration input for the type parameter. Possible values are: • 1 for hour • 2 for day • 3 for week • 4 for month By default, this is set to 3.
type	Optional for /indicators/upload	Integer	Indicates the type of the timestamp to use. You can use

			either started_by or ending_by options. Possible values are: • 1 to filter the results based on starting (filters the events till the timestamp given) • 2 to filter the results based on ending (filters results starting from the timestamp given) By default, this is set to 2.
date	Optional for /indicators/upload	String	Represents the date for filtering the results for the type parameter. The format is (YYYY-MM-DD).

Example response


```
    {
      "status": "success",
      "message": "Successfully fetched the results through the hunt",
      "data": {
        "count": 1,
        "results": [
          {
            "pid": "4752",
            "uuid": "EC2CE2E2-3D74-1248-2FA9-23F2E960ED42",
            "version": "4.0.2",
            "watcher": "-1",
            "extensions": "active",
            "start_time": "1592672947",
            "config_hash": "71f4969da7d79f6b2cbeb64d02e04b17bd8815e7",
            "instance_id": "78a850bf-844e-426a-8cc6-a66d3975a2ba",
            "build_distro": "10",
            "config_valid": "1",
            "build_platform": "windows"
          }
        ]
      }
}
```


Export hunt results

Use this API to export results (to a CSV file) from a completed hunt.

URL

/hunt-upload/export

/indicators/upload/export

Request type

POST

Example payload format

```
{
  "file": <file of indicators>,
  "type": "md5",
  "host_identifier": "EC2300D6-B0D5-F9A6-1237-6553106EC525",
  "query_name": "win_file_events"
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
file	Required for /hunt-upload/export and /indicators/upload/export	File	Provides a file containing a list of indicators. Each indicator in the file is separated by a new line.
type (for /hunt-upload/export) indicator_type (for /indicators/upload/export)	Required for both	String	Indicates the type of hunt to perform. Possible values are: • md5 • sha256 • domain_name • ja3_md5 • process_guid • parent_process_guid • target_path • target_name • process_name • remote_address
host_identifier	Required for /hunt-upload/export Optional for /indicators/upload/export	String	Specifies the identifier of the host.
query_name	Required for /hunt-upload/export Optional for /indicators/upload/export	String	Specifies the name of the query to filter the results.
duration	Optional for /indicators/upload/export	Integer	Specifies the duration input for the type

	Not applicable for /hunt-upload/export		parameter. Possible values are: • 1 for hour • 2 for day • 3 for week • 4 for month By default, this is set to 3.
type	Not applicable for /hunt-upload/export Optional for /indicators/upload/export	Integer	Indicates the type of the timestamp to use. You can use either started_by or ending_by options. Possible values are: • 1 to filter the results based on starting (filters the events till the timestamp given) • 2 to filter the results based on ending (filters results starting from the timestamp given) By default, this is set to 2.
date	Not applicable for /hunt-upload/export Optional for /indicators/upload/export	String	Represents the date for filtering the results for the type parameter. The format is (YYYY-MM-DD).

Hunt results using a list of indicators

Use this API to fetch the data from multiple hosts by using a list of indicators. In an API call, you can hunt for only one type of indicator. The API results are returned in JSON format.

URL

/indicators/hunt

Request type

POST

Format 1

Example payload

```
{
  "indicators": "275a71899f7db9d1663fc695ec2fe2a2c4538,
275a71899fdjsaddb9d1663fc695ec2fe2a2c453fsgs",
  "type": "md5"
```

}

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
indicators	Required	String	Provides a list of one or more indicators. When specifying multiple values, separate each indicator with a comma.
type	Required	String	Indicates the type of hunt to perform. Possible values are: • md5 • sha256 • domain_name • ja3_md5 • process_guid • parent_process_guid • target_path • target_name • process_name • remote_address

Example response


```
{
  "status": "success",
  "message": "Successfully fetched the results through the hunt",
  "data": [
    {
      "hostname": "host_1",
      "host_identifier": "host_ID",
      "queries": [
        {
          "query_name": "osquery_info",
          "count": 1
        }
      ]
    }
  ]
}
```


Format 2

Example payload


```
{
  "indicators": "275a71899f7db9d1663fc695ec2fe2a2c4538,
275a71899fdjsaddb9d1663fc695ec2fe2a2c453fsgs",
  "type": "md5",
  "host_identifier": "EC2300D6-B0D5-F9A6-1237-6553106EC525",
  "query_name": "win_file_events",
  "start": 2,
  "limit": 10
```

}

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
indicators	Required	String	Provides a list of one or more indicators. Each indicator in the string is separated by a comma.
type	Required	String	Indicates the type of hunt to perform. Possible values are: • md5 • sha256 • domain_name • ja3_md5 • process_guid • parent_process_guid • target_path • target_name • process_name • remote_address
host_identifier	Required	String	Specifies the identifier of the host.
query_name	Required	String	Specifies the name of the query to filter the results.
start	Optional	Integer	Specifies the start value of the results. This value is use for pagination. By default, this is set to 0.
limit	Optional	Integer	Specifies the end value of the results. This value is use for pagination. By default, this is set to 10.

Example response


```
{
  "status": "success",
  "message": "Successfully fetched the results through the hunt",
  "data": {
    "count": 1,
    "results": [
      {
        "pid": "4752",
        "uuid": "EC2CE2E2-3D74-1248-2FA9-23F2E960ED42",
        "version": "4.0.2",
        "watcher": "-1",
```

```
        "extensions": "active",
        "start_time": "1592672947",
        "config_hash": "71f4969da7d79f6b2cbeb64d02e04b17bd8815e7",
        "instance_id": "78a850bf-844e-426a-8cc6-a66d3975a2ba",
        "build_distro": "10",
        "config_valid": "1",
        "build_platform": "windows"
      }
    ]
  }
}
```


Search

This section describes APIs that help in managing searches.

Limited column search in query results

Use this API to fetch result data for limited columns only from multiple hosts. This API allows you perform a search based on different criteria, such as query name, host ID, and columns specified in JSON format. Here is the list of columns you can search on:

- md5
- sha256
- domain_name
- ja3_md5
- process_guid
- parent_process_guid
- target_path
- target_name
- process_name
- remote_address

We recommend you use this API for searches because fetching data only from limited or indexed columns offers performance benefits.

URL

/activity/search

Request type

POST

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
conditions	Required	JSON	Specifies the conditions on which to search to narrow down the fetched results.

host_identifier	Optional	String	Specifies the host identifier of the node. Provide a value to filter and fetch results only for the specified host.
query_name	Optional	String	Specifies the name of a query. Provide a value to filter and fetch results only for the specified query.
start	Optional	Integer	Specifies the start value of the results. This value is use for pagination. By default, this is set to 0.
limit	Optional	Integer	Specifies the end value of the results. This value is use for pagination. By default, this is set to 10.
duration	Optional	Integer	Specifies the duration input for the type parameter. Possible values are: • 1 for hour • 2 for day • 3 for week • 4 for month By default, this is set to 3.

Example payload format

```
{
  "conditions": {
    "condition": "OR",
    "rules": [
      {
        "id": "name",
        "field": "name",
        "type": "string",
        "input": "text",
        "operator": "contains",
        "value": "EC2"
      },
      {
        "id": "name",
        "field": "name",
        "type": "string",
        "input": "text",
        "operator": "equal",
        "value": "pc"
      }
    ],
    "valid": true
```

```
    },
    "host_identifier": "EC241E83-BDC2-CAFC-BF9F-28C22B37A7F0",
    "query_name": "per_query_perf",
    "start": 2,
    "limit": 2,
    "duration": "3",
    "date": "2020-8-5",
    "type": "2"
}
```


Example response format


```
{
  "status": "success",
  "message": "Successfully fetched the results through the search",
  "data": {
    "count": 28,
    "results": [
      {
        "id": 172270780,
        "name": "process_events",
        "timestamp": "19-10-2020 10:10:47.000000",
        "action": "added",
        "columns": {
          "cwd": "\"/var/backups\"",
          "eid": "0000023296",
          "gid": "0",
          "pid": "2625",
          "uid": "0",
          "auid": "4294967295",
          "egid": "0",
          "euid": "0",
          "path": "/usr/bin/python3.6",
          "time": "1603102243",
          "ctime": "1602831478",
          "parent": "2619",
          "cmdline": "/usr/bin/python3 -Es /usr/bin/lsb_release -i -s"
        },
        "node_id": 60,
        "uuid": "41184ad2-f651-4b9d-baff-f201fc38ce76",
        "status": 0,
        "task_id": null,
        "hostname": "host_1",
        "host_identifier": "host_ID"
      }
    ]
  }
}
```


Search all query results

Use this API to fetch data from multiple hosts based on specified search criteria (in JSON format). There ais no limitation on the columns you can specify for the search.

We recommend you use caution when using this API. If you perform an exhaustive search or search based on a considerable number of columns, this API may cause some performance degradation.

URL

/search

Request type

POST

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
conditions	Required	JSON	Specifies the conditions on which to search to narrow down the fetched results.
host_identifier	Optional	String	Specifies the host identifier of the node. Provide a value to filter and fetch results only for the specified host.
query_name	Optional	String	Specifies the name of a query. Provide a value to filter and fetch results only for the specified query.
start	Optional	Integer	Specifies the start value of the results. This value is use for pagination. By default, this is set to 0.
limit	Optional	Integer	Specifies the end value of the results. This value is use for pagination. By default, this is set to 10.

Format 1

Example payload

```
{
  "conditions": {
    "condition": "OR",
    "rules": [
      {
        "id": "name",
        "field": "name",
        "type": "string",
        "input": "text",
        "operator": "contains",
        "value": "EC2"
      },
      {
        "id": "name",
        "field": "name",
```

```
            "type": "string",
            "input": "text",
            "operator": "equal",
            "value": "pc"
          }
        ],
        "valid": true
      }
}
```


Required payload parameters

Conditions

Example response


```
    {
      "status": "success",
      "message": "Successfully fetched the results through the payload
    given",
      "data": [
        {
          "hostname": "host_1",
          "host_identifier": "host_ID",
          "queries": [
            {
              "query_name": "osquery_info",
              "count": 1
            }
          ]
        }
      ]
}
```


Format 2

Example payload


```
    {
      "conditions": {
        "condition": "OR",
        "rules": [
          {
            "id": "name",
            "field": "name",
            "type": "string",
            "input": "text",
            "operator": "contains",
            "value": "EC2"
          },
          {
            "id": "name",
            "field": "name",
            "type": "string",
            "input": "text",
```

```
            "operator": "equal",
            "value": "pc"
          }
        ],
        "valid": true
      },
      "host_identifier": "EC241E83-BDC2-CAFC-BF9F-28C22B37A7F0",
      "query_name": "per_query_perf",
      "start": 2,
      "limit": 2
}
```


Required payload parameters

conditions, host_identifier, query_name, start and limit

Example response


```
    {
      "status": "success",
      "message": "Successfully fetched the results through the payload
    given",
      "data": {
        "count": 1,
        "results": [
          {
            "pid": "4752",
            "uuid": "EC2CE2E2-3D74-1248-2FA9-23F2E960ED42",
            "version": "4.0.2",
            "watcher": "-1",
            "extensions": "active",
            "start_time": "1592672947",
            "config_hash": "71f4969da7d79f6b2cbeb64d02e04b17bd8815e7",
            "instance_id": "78a850bf-844e-426a-8cc6-a66d3975a2ba",
            "build_distro": "10",
            "config_valid": "1",
            "build_platform": "windows"
          }
        ]
      }
}
```


Export query results

Use this API to export data (in CSV format) for a host and query combination.

The /schedule_query/export API is deprecated and no longer available. Use the /hosts/search/export API instead.

Response

This section describes APIs that help in managing response actions. All APIs detailed in this section are available only in the Enterprise Edition of EclecticIQ Endpoint Response and unavailable in the Community Edition.

Get a list of all response actions

Use this API to fetch a list of all response actions taken against the managed agents from the EclecticIQ Endpoint Response server.

URL

/response

Request type

POST

Example payload format

```
{
  "start": 0,
  "limit": 1,
  "searchterm": "pol"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
start	Optional	Integer	Specifies the start value of the results. This value is use for pagination. By default, this is set to 0.
limit	Optional	Integer	Specifies the end value of the results. This value is use for pagination. By default, this is set to 10.
searchterm	Optional	String	Specifies the term to filter the search results. Only results containing the searchterm are returned.
column	Optional	String	Specifies the name of the column based on which to sort the results. This is used in conjunction with order_by. Possible value is created_at.
order_by	Optional	String	Specifies how to sort the results. This is used in conjunction with column.

			Possible values are asc (for ascending) and desc (for descending).

Example response format


```
{
  "status": "success",
  "message": "Successfully fetched the responses info",
  "data": {
    "count": 1,
    "total_count": 1,
    "results": [
      {
        "id": 7,
        "action": "stop",
        "command": {
          "action": "stop",
          "actuator": {
            "endpoint": "polylogyx_vasp"
          },
          "target": {
            "process": {
              "name": "calc.exe",
              "pid": "8282"
            }
          }
        },
        "created_at": "2020-08-04 15:10:11.284031",
        "updated_at": "2020-08-04 15:10:11.283453",
        "script_name": null,
        "target": "process",
        "Executed": "1/1"
      }
    ]
  }
}
```


Export all response actions

Use this API to export (to a CSV file) all the response actions taken against the managed agents.

URL

/response/export

Request type

POST

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*

host_identifier	Optional	String	Specifies the host identifier of the node.

Get additional information for all response actions

Use this API to fetch a list of all response actions along with details of the hosts on which the action was taken and the result of the response action.

URL

/response/view

Request type

POST

Example payload format

```
{
  "start": 0,
  "limit": 1,
  "searchterm": "EC2",
  "openc2_id": 1
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
start	Optional	Integer	Specifies the start value of the results. This value is use for pagination. By default, this is set to 0.
limit	Optional	Integer	Specifies the end value of the results. This value is use for pagination. By default, this is set to 10.
searchterm	Optional	String	Specifies the term to filter the search results. Only results containing the searchterm are returned.
openc2_id	Required	Integer	Specifies the response action ID.

Example response format

```
{
  "status": "success",
  "message": "Successfully fetched the responses info",
  "data": {
    "count": 1,
    "total_count": 7,
    "results": [
      {
        "id": 8,
        "command": {
```

```
            "action": "stop",
            "actuator": {
              "endpoint": "polylogyx_vasp"
            },
            "target": {
              "process": {
                "name": "calc.exe",
                "pid": "8282"
              }
            }
          },
          "created_at": "2020-08-04 15:10:11.315204",
          "updated_at": "2020-08-04 15:10:11.288915",
          "node_id": 3,
          "command_id": "2c92808273b870760173ba05d560000c",
          "status": "failure",
          "message": "RESP_SERVER_DISABLED",
          "hostname": "host_1",
          "target": "process",
          "action": "stop"
        }
      ]
    }
}
```


Get a response action

Use this API to fetch or view information for a specific response action. This API also returns the execution status of the response action.

URL

/response/<command_id>

Request type

GET

Example response format


```
{
  "status": "success",
  "message": "Successfully received the command status",
  "data": {
    "id": 8,
    "command": {
      "action": "stop",
      "actuator": {
        "endpoint": "polylogyx_vasp"
      },
      "target": {
        "process": {
          "name": "calc.exe",
          "pid": "8282"
```

```
          }
        }
      },
      "created_at": "2020-08-04 15:10:11.315204",
      "updated_at": "2020-08-04 15:10:11.288915",
      "node_id": 3,
      "command_id": "2c92808273b870760173ba05d560000c",
      "status": "failure",
      "message": "RESP_SERVER_DISABLED",
      "hostname": "host_1",
      "target": "process",
      "action": "stop"
    }
  }
```


Get connection status for all hosts

Use this API to fetch response action connection status for all hosts.

- An online connection indicates that the host is ready to accept an action from EclecticIQ Endpoint Response server.
- An offline connection indicates the host is unavailable (possibly shut down).

URL

/response/status/all

Request type

GET

Example response format


```
  {
    "status": "success",
    "message": "Successfully fetched the response action status of all
  hosts",
    "data": [
      {
        "hostIdentifier": "ec2bff15-e870-567a-0ed2-3642bcbaf257",
        "epName": "ip-172-31-10-241",
        "onlineStatus": "ONLINE",
        "responseEnabled": true,
        "endpointOnline": true,
        "host_degraded": false
      },
      {
        "hostIdentifier": "ec27bfa3-bbb1-f25f-f695-21ed19e5b62b",
        "epName": "ip-172-31-17-167",
        "onlineStatus": "ONLINE",
        "responseEnabled": true,
        "endpointOnline": false,
        "host_degraded": true
      }
```

```
    ]
}
```

Get connection status for a host

Use this API to fetch response action connection status for a specific host.

- An online connection indicates that the host is ready to accept an action from EclecticIQ Endpoint Response server.
- An offline connection indicates the host is unavailable (possibly shut down).

URL

/response/status

Request type

POST

Example payload format

```
{
  "host_identifier": "EC2CD1A0-140B-9331-7A60-CFFCE29D2E71",
  "node_id": 1
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
host_identifier	Required if node_id is not specified	String	Specifies the identifier of the host.
node_id	Required if host_identifier is not specified	Integer	Specifies the node identifier of the host.

Example response format

```
{
  "status": "success",
  "message": "Successfully received the status",
  "responseEnabled": true,
  "endpointOnline": true
}
```

Restart an agent

Use this API to restart an agent by sending a response action.

URL

/response/restart-agent

Request type

POST

Example payload format

```
{
  "host_identifier": "EC2CD1A0-140B-9331-7A60-CFFCE29D2E71"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
host_identifier	Required	String	Specifies the host identifier for the node to restart.

Example response format

```
{
  "status": "success",
  "message": "Action to restart agent is added successfully"
}
```

Initiate a response action

Use this API to take an action on an endpoint. Using this API, you can stop a process, delete a file, or create or update network rules.

URL

/response/add

Request type

POST

Example payload format

File Response Action	<pre>{
	  "action": "delete",
	  "actuator_id": "EC2CD1A0-140B-9331-7A60-CFFCE29D2E71",
	  "target": "file",
	  "file_name": "C:\\Users\\PolyLogyx\\Downloads\\suspicious.exe",
	  "file_hash": "o2MJjT8UKSRM7eoLDMWvm4LxqaFvDxd2wLg1KQQQ2jXfG5UE"
	}</pre>

Process Response Action	<pre>{
	  "action": "stop",
	  "actuator_id": "EC2CD1A0-140B-9331-7A60-CFFCE29D2E71",
	  "target": "process",
	  "process_name": "suspicious1.exe",
	  "pid": "3123"
	}</pre>

Network Response Action	Delete a rule	<pre>{
		  "action": "delete",
		  "actuator_id": "EC2CD1A0-140B-9331-7A60-CFFCE29D2E71",
		  "target": "ip_connection",
		  "rule_name": "test_rule_12"
		}</pre>

	Isolate a rule	<pre>{
		  "action": "contain",
		  "actuator_id": "EC2CD1A0-140B-9331-7A60-CFFCE29D2E71",
		  "target": "ip_connection",
		  "rule_name": "test_rule_12",
		  "rule_group": "test",
		  "src_port": "",
		  "dst_port": "",
		  "dst_addr": "",
		  "application": "",
		  "direction": "1",
		  "layer4_protocol": "256"
		}</pre>

Payload parameters

Parameter	***Data type***	***Description***
target	String	Specifies the type of action to take. Possible values are: • file • process • ip_connnection
actuator_id	String	Specifies one or more host IDs (comma separated) to indicate the hosts on which to take the action.
tags	String	Specifies one or more tags (comma separated) to consider for the response action. All hosts assigned the specified tags are considered for the response action.
os_name	String	Specifies one or more operating systems (comma separated). All hosts running the specified operating systems are considered for the response action.
action	String	Specifies the response action to take to initiate. Possible values are delete, stop, and contain.
file_name	String	Specifies the file name of the file to delete.
file_hash	String	Specifies the file hash of the file to delete.

process_name	String	Specifies the full path of the process to terminate.
pid	String	Specifies the process ID of the process to terminate.
rule_name	String	Provides the network rule name to update to the Windows firewall.
rule_group	String	Provides the network rule group to update to the Windows firewall.
rule_description	String	Provides a description for the network rule.
src_port	String	Specifies the source port to use in the network rule to isolate. You can specify a range or a value. Possible values can be between 1 and 65535.
dst_port	String	Specifies the destination port to use in the network rule to isolate. You can specify a range or a value. Possible values can be between 1 and 65535.
dst_addr	String	Specifies the destination address to use in the network rule to isolate. You can specify a range or a value.
application	String	Specifies the program name. You can specify an absolute or relative path to the application.
direction	String	Specifies whether the rule is an inbound rule or outbound rule. Possible values are 1 (in) and 2 (out). By default, this is set to 1.
layer4_protocol	String	Specifies the request protocol type to use. Possible values are 2 (any), 6 (TCP), and 17 (UDP). By default, this is set to 2.

Required payload parameters

File Response Action		action, actuator_id, file_name/file_hash and target
Process Response Action		action, actuator_id, process_name/pid and target
Network Response Action	Delete a rule	action, actuator_id, rule_name and target
	Isolate a rule	action, actuator_id, rule_name, rule_group, rule_description, src_port, dst_port, dst_addr, application, and target

Example response format

```
{
  "status": "success",
  "message": "Successfully sent the response command",
  "command_id": "2c92808a69099f17016910516100000a"
}
```

Initiate a custom action

Use this API to initiate a custom action for one or more hosts.

You can pass script content directly to the API. Typically, shell scripts are used for the Linux and macOS operating systems while batch or PowerShell scripts are used for the Windows operating system.

URL

/response/custom-action

Request type

POST

Example payload format

```
{
  "host_identifier": "EC2CD1A0-140B-9331-7A60-CFFCE29D2E71",
  "content": "dir\n$pwd",
  "file_type": "4",
  "save_script": "true",
  "script_name": "dir_script"
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
host_identifier	Required	String	Specifies one or more host identifiers (comma separated) for the nodes on which to take the action.
tags	Optional	String	Specifies one or more tags (comma separated) to identify the hosts on which to take the action. The action is sent to all hosts with the specified tags.
os_name	Optional	String	Specifies one or more operating systems (comma separated) to identify the hosts on which to take the action. The action is sent to all hosts running the specified operating systems.

content	Required	String	Provides the content of the script file to run.
file_type	Required	integer	Specifies the type of script file to run. Possible values are: • 1 for .bat files • 2 for PowerShell scripts • 4 for shell scripts
file	Optional	File	Provides the script file to run.
save_script	Optional	String	Specifies whether to save the script file to the EclecticIQ Endpoint Response server database. Possible values are: • true to save the script • false to not save the script
params	Optional	String	Specifies parameters for the script file to run.
script_name	Optional	String	Provides a name for the script file.

Example response format

```
{
  "status": "success",
  "message": "Action is added successfully",
  "openc2_id": 1
}
```

Delete response actions

Use this API to delete one or more response actions from the list on the EclecticIQ Endpoint Response server.

URL

/response/delete

Request type

DELETE

Example response format

```
{
  "openc2_ids": "1,2"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
openc2_ids	Required	String	Specifies the response action IDs to delete. When specifying multiple values, separate each value using a comma.

Example response format

```
{
  "status": "success",
  "message": "Successfully removed the action"
}
```

Delete a response action

Use this API to delete a completed response action from the actions list on the EclecticIQ Endpoint Response server.

URL

/response/<openc2_id>/delete

Request type

DELETE

Example response format

```
{
  "status": "success",
  "message": "Successfully removed the response"
}
```

Cancel an ongoing response action

Use this API to stop or cancel an ongoing action. Stopping refers to preventing further execution on an agent; the processed or executed part of the script cannot be reversed.

URL

/response/cancel

Request type

POST

Example payload format

```
{
  "command_id": "2c92808478ca277b0178ca2b9ef80005"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
command_id	Required	String	Specifies the command ID for the action to cancel.

Example response format

```
{
  "status": "success",
  "message": "Successfully sent command to cancel action"
}
```

Initiate a live response action

Use this API to initiate a live response action. You can send any shell, bash, batch, or PowerShell command based on its platform. The executed response data can be captured through a WebSocket connection.

URL

/response/live_response

Request type

POST

Example payload format

```
{
  "host_identifier": "EC2EBD16-8D48-0C24-EB42-B22333D7F08D",
  "content": "dir\n$pwd",
  "file_type": "2",
  "file": "",
  "save_script": "true",
  "script_name": "dir_script"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
host_identifier	Required	String	Specifies the host identifier for the node on which to take the action.
content	Optional	String	Provides the content of the script file to run.
file_type	Required	integer	Specifies the type of script file to run. Possible values are: • 1 for .bat files • 2 for PowerShell scripts • 4 for shell scripts

file	Optional	File	Provides the script file to run.
save_script	Optional	String	Specifies whether to save the script file to the EclecticIQ Endpoint Response server database. Possible values are: • true to save the script • false to not save the script
params	Optional	String	Specifies parameters for the script file to run.
script_name	Optional	String	Provides a name for the script file.

Example response format

```
{
  "openc2_id": 133,
  "command_id": "2c92808478edeff20178ee8f18910025",
  "message": "Action is added successfully",
  "status": "success"
}
```

Get query results

1. Make a connection from a web socket client to one of the following URLs.

```
wss://<server_IP>/esp-ui/distributed/result
wss://<server_IP>/esp-ui/websocket/distributed/result
```

2. Send the received query_id to the socket server.
3. Ensure the socket client listen to server till a message is received.
4. Close the web socket connection after receiving results.

Windows Defender

This section describes APIs that help in configuring and using the Windows Defender application. These APIs are available only for endpoints running the Windows operating system. All APIs detailed in this section are available only in the Enterprise Edition of EclecticIQ Endpoint Response and unavailable in the Community Edition.

Initiate a scan for a host

Use this API to trigger an immediate scan on a host using the Windows Defender application.

Note: You can invoke this API multiple times because it does not retain the state of the previous command sent.

URL

/defender-management/scan-now

Request type

POST

Example payload format

```
{
  "host_identifier": "EC27FE09-DEBD-F637-E17C-63CDCBF640DB",
  "scan_type": 1,
  "file_path": ""
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
host_identifier	Required	String	Specifies the host identifier for the node.
scan_type	Required	String	Specifies the type of scan to run. Possible values are 1 (quick scan), 2 (full scan), and 3 (custom scan).
file_path	Optional; Required if you specify a value of 3 for the scan_type parameter.	String	Specifies the path to the file or directory to scan.

Example response format

```
{
  "openc2_id": 77,
  "message": "Action is added successfully",
  "status": "success"
}
```

Schedule a scan for a host

Use this API to schedule a scan on a host using the Windows Defender application.

URL

/defender-management/schedule-scan

Request type

POST

Example payload format

```
{
  "host_identifier": "EC27FE09-DEBD-F637-E17C-63CDCBF640DB",
  "scan_type": 1,
  "time": "hh:mm",
  "scan_day": "21-04-2021"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
host_identifier	Required	String	Specifies the host identifier for the node.
scan_type	Required	String	Specifies the type of scan to run. Possible values are 1 (quick scan) and 2 (auto trigger scan).
time	Required	String	Indicate the time at which to scan.
scan_day	Optional	String	Specifies the day on which to run the auto trigger scan. Possible values are 0 through 8. • 0 - Everyday • 1 - Sunday • 2 - Monday • 3 - Tuesday • 4 - Wednesday • 5 - Thursday • 6 - Friday • 7 - Saturday • 8 - Never

Example response format

```
{
  "openc2_id": 77,
  "message": "Action is added successfully",
  "status": "success"
}
```

Check protection updates for a host

Use this API to fetch protection updates (including updates and security intelligence version) from the Windows Defender application.

URL

/defender-management/check-update

Request type

POST

Example payload format

```
{
  "host_identifier": "EC27FE09-DEBD-F637-E17C-63CDCBF640DB"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
host_identifier	Required	String	Specifies the host identifier for the node.

Example response format

```
{
  "openc2_id": 77,
  "message": "Action is added successfully",
  "status": "success"
}
```

Configure scan settings for a host

Use this API to configure the Windows Defender application for the agent. You can specify the items to exclude from scanning.

URL

/defender-management/configure

Request type

POST

Example payload format

```
{
  "host_identifier": "EC27FE09-DEBD-F637-E17C-63CDCBF640DB",
  "file_type": ".txt",
  "path": "c://",
  "process": "notepad.exe",
  "action": "add/remove"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
host_identifier	Required	String	Specifies the host identifier for the node.
action	Required	String	Indicates whether to add or remove the file, path, or process from the exclusion list. Possible values are add and remove.
file_type	Required, if process or path is not specified	String	Specifies the file type or file extension to exclude for scanning.
path	Required, if process or	String	Specifies the path of the file or directory to exclude for scanning.

	file_type is not specified		
process	Required, if path or file_type is not specified	String	Indicates the name of the process to exclude for scanning.

Example response format

```
{
  "message": "Action is added successfully",
  "status": "success"
}
```

View scan settings for a host

Use this API to fetch the current Windows Defender configuration, such as excluded paths and scanning options.

URL

/defender-management/current-settings

Request type

POST

Example payload format

```
{
  "host_identifier": "EC27FE09-DEBD-F637-E17C-63CDCBF640DB"
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
host_identifier	Required	String	Specifies the host identifier for the node.

Example response format

```
{
  "openc2_id": 77,
  "message": "Action is added successfully",
  "status": "success"
}
```

Review threat details for a host

Use this API to fetch the current threat details, if any, for a host from the Windows Defender application. The details indicate if a host is safe from attacks and provide a count of files scanned.

URL

/defender-management/computer-status

Request type

POST

Example payload format

```
{
  "host_identifier": "EC27FE09-DEBD-F637-E17C-63CDCBF640DB"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
host_identifier	Required	String	Specifies the host identifier for the node.

Example response format

```
{
  "openc2_id": 77,
  "message": "Action is added successfully",
  "status": "success"
}
```

Review quarantined threats for a host

Use this API to fetch all the threats quarantined for a host by the Windows Defender application.

URL

/defender-management/get-quarantine

Request type

POST

Example payload format

```
{
  "host_identifier": "EC27FE09-DEBD-F637-E17C-63CDCBF640DB"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
host_identifier	Required	String	Specifies the host identifier for the node.

Example response format

```
{
  "openc2_id": 77,
  "message": "Action is added successfully",
  "status": "success"
}
```

Get application status for a host

Use this API to fetch the status of the Windows Defender application for a host. The status indicates if the application is switched off or is on and protecting the host.

URL

/defender-management/status_refresh

Request type

POST

Example payload format

```
{
  "host_identifier": "EC27FE09-DEBD-F637-E17C-63CDCBF640DB"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
host_identifier	Required	String	Specifies the host identifier for the node.

Example response format

```
{
  "openc2_id": 77,
  "message": "Action is added successfully",
  "status": "success"
}
```

Carve a quarantined file for a host

Use this API to initiate a carve for a quarantined file. Carving occurs only if the file is present.

URL

/defender-management/quarantine_file/carve

Request type

POST

Example payload format:

```
{
  "host_identifier": "EC27FE09-DEBD-F637-E17C-63CDCBF640DB"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
host_identifier	Required	String	Specifies the host identifier for the node.

path	Required	String	Specifies the full path of the quarantined file to carve.

Example response format

```
{
  "message": "carve query has been sent to the host",
  "status": "success"
}
```

Users

This section describes APIs that help in managing users.

Get a list of all users

Use this API to fetch a list of all users added to the EclecticIQ Endpoint Response server. This API also returns additional user information, such as status, SSO login status, and assigned role.

URL

/users

Request type

GET

Example payload format

```
{
  "start": 0,
  "limit": 10,
  "searchterm": "te"
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
start	Optional	Integer	Specifies the start value of the results. This value is use for pagination. By default, this is set to 0.
limit	Optional	Integer	Specifies the end value of the results. This value is use for pagination. By default, this is set to 10.
searchterm	Optional	String	Specifies the term to filter the search results. Only results containing the searchterm are returned.

status	Optional	Boolean	Specifies the user status based on which to filter the search results. Possible values are true and false. Specify a value of true to fetch results for active users and false to fetch results for inactive users.
role	Optional	String	Specifies the user role based on which to filter the search results. Possible values are admin and analyst.
column	Optional	String	Specifies the name of the column based on which to sort the results. This is used in conjunction with order_by. Possible values username.
order_by	Optional	String	Specifies how to sort the results. This is used in conjunction with column. Possible values are asc (for ascending) and desc (for descending).

Example response format


```
{
  "status": "success",
  "message": "All users information has been fetched successfully",
  "data": {
    "results": [
      {
        "id": 1,
        "username": "admin",
        "first_name": "",
        "last_name": "",
        "email": "admin@example.com",
        "status": true,
        "enable_sso": true,
        "roles": [
          "admin"
        ]
      }
    ],
    "count": 1,
    "total_count": 1
  }
}
```


Create a user

Use this API to create a new user for the EclecticIQ Endpoint Response platform. Only administrators can create new users.

URL

/users

Request type

POST

Example payload format

```
{
  "username": "analyst1",
  "first_name": "analyst",
  "last_name": "analyst",
  "password": "Test@1234",
  "email": "analyst@example.com",
  "role": "analyst",
  "enable_sso": true
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
username	Required	String	Specifies the username of the user to add.
email	Required	String	Specifies the user email.
password	Required	String	Specifies the password for the user.
first_name	Optional when using EclecticIQ Endpoint Response 3.5.1 Required when using EclecticIQ Endpoint Response 4.0.0	String	Provides the first name for the user.
last_name	Optional	String	Provides the last name for the user.
role	Required	string	Indicate the role to be assigned to the user. Possible values are analyst and admin.
enable_sso	Optional	Boolean	Indicates whether to allow the user to use SSO to login. Possible values are true and false. Providing a value of true to enable SSO login for the use. By default, this is set to false.

Example response format

```
{
  "status": "success",
```

```
  "message": "User 'analyst1' has been created successfully"
}
```

Assign role to users

Use this API to assign a role (analyst or administrator) to one or more users. This operation can be performed only by user with administrator privileges (admin role assigned).

URL

/users

Request type

PUT

Example payload format

```
{
  "username": "analyst1,analyst2",
  "role": "analyst"
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
username	Required	Array	Specifies one or more usernames (comma separated) for the users to update.
role	Required	String	Indicates the role to be assigned to the users. Possible values are analyst and admin.

Example response format

```
{
  "status": "success",
  "message": "Users have been assigned with role 'analyst'
successfully"
}
```

Get information for a user

Use this API to fetch information, such as first name, last name, username, and email for a specific user or for self. To do this for a different user, you must have administrative privileges.

URL

/users/user/<user_id>

/users/me

Request type

GET

Example response format

```
{
  "status": "success",
  "message": "User '<User 7>' information has been fetched
successfully",
  "data": {
    "id": 7,
    "username": "analyst1",
    "first_name": "analyst",
    "last_name": "analyst",
    "email": "analyst@example.com",
    "status": true,
    "enable_sso": true,
    "roles": [
      "analyst"
    ]
  }
}
```

Update details for a user

Use this API to edit information (such as first name, last name, username, and email) for a specific user or for self. To do this for a different user, you must have administrative privileges.

URL

/users/user/<user_id>

/users/me

Request type

PUT

Example payload format

```
{
  "new_user_name": "analyst1",
  "first_name": "analyst",
  "last_name": "analyst",
  "email": "analyst@example.com",
  "role": "analyst",
  "status": true,
  "enable_sso": true
}
```

Payload parameters

Parameter	***Parameter Type***	***Data type***	***Description***
email	Required	String	Specifies the user email.
new_user_name	Optional	String	Provides the new username for the user.

first_name	Optional	String	Provides the first name for the user.
last_name	Optional	String	Provides the last name for the user.
role	Required	string	Indicates the role to be assigned to the user. Possible values are analyst and admin.
status	Optional	Boolean	Indicates whether to allow the user to login. Possible values are true and false. Providing a value of false deactivates the account and prevents the user from logging in. By default, this is set to false.
enable_sso	Optional	Boolean	Indicates whether to allow the user to use SSO to login. Possible values are true and false. Providing a value of true to enable SSO login for the use. By default, this is set to false.

Example response format

```
{
  "status": "success",
  "message": "User's info has been updated successfully"
}
```

Get activity details for a user

Use this API to fetch details of details of the activities performed by one or more users on the EclecticIQ Endpoint Response platform. To fetch activity details for a specific user, apply filters (based on the user_id).

This operation can only be performed by a user with administrator privileges (admin role assigned to user).

URL

/users/platform_activity

Request type

GET

Example payload format

```
{
  "start": 0,
  "limit": 10,
  "searchterm": "An"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
user_id	Optional	Integer	Specifies the user ID of the user for whom to fetch activity details.
start	Optional	Integer	Specifies the start value of the results. This value is use for pagination. By default, this is set to 0.
limit	Optional	Integer	Specifies the end value of the results. This value is use for pagination. By default, this is set to 10.
searchterm	Optional	String	Specifies the term to filter the search results. Only results containing the searchterm are returned.

Example response format


```
{
  "status": "success",
  "message": "Successfully fetched the latest user(s) platform
activity",
  "data": {
    "count": 435,
    "total_count": 435,
    "results": [
      {
        "id": 168572,
        "action": "updated",
        "text": null,
        "user": {
          "id": 1,
          "first_name": "",
          "last_name": "",
          "username": "admin"
        },
        "created_at": "2022-02-23 11:18:35.688223",
        "item": {
          "type": "Settings",
          "id": 1,
          "name": "er_ui_log_level"
        }
      }
    ]
  }
}
```

Passwords

This section describes APIs that help in managing passwords.

Reset a user's password

Use this API to reset the password for a user. This operation can only be performed by a user with administrator privileges (admin role assigned).

After the user logs into platform with the password created by administrator, the user is asked to change the password.

URL

/users/user/<user_id>/password

Request type

PUT

Example payload format

```
{
  "new_password": "Analyst@1234"
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
new_password	Required	String	Specifies the new user password.

Example response format

```
{
  "status": "success",
  "message": "Password is updated successfully"
}
```

Change your password

Use this API to change your existing login password for the EclecticIQ Endpoint Response server.

URL

/users/me/password

Request type

PUT

Example payload format

```
{
  "old_password": "Analyst@123",
  "new_password": "Analyst@1234",
  "confirm_new_password": "Analyst@1234"
```

```
}
```

Payload parameters

Parameter	*Parameter Type*	*Data type*	*Description*
old_password	Required	String	Represents the old user password.
new_password	Required	String	Specifies the new user password.
confirm_new_password	Required	String	Specifies the new user password.

Example response format

```
{
  "status": "success",
  "message": "Password is updated successfully"
}
```