Fortinet Endpoint Protection and Response Platform RESTful API

Version 5.0 Rev 3

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

October 2023

Fortinet Endpoint Protection and Response Platform RESTful API

Table of Contents

Change Log

Date	Change Description
March 2021	Initial release
December 2021	Version 5.0.3 SP1 New APIs: • audit/get-audit • playbooks-policies/map-connectors-to-actions • playbooks-policies/set-action-classification • threat-hunting-settings/assign-collector-groups Modified APIs: • events/list-events new output parameter: threatDetails. • events/list-raw-data-items new output parameter: remediateDevice. • administrator/list-system-summary new output parameter: repositoryAddOns and modified output parameters: licenseFeatures and licenseType. • organizations/list-organizations new output parameters: eXtendedDetection and repositoryAddOns • users/update-saml-settings modified input parameter localAdminGroupName (was adminsGroupName) • users/delete-saml-settings modified input parameter: organization (was organizationName) • threat-hunting/search modified input parameter: pageNumber (was offset) • threat-hunting/facets modified input parameter: pageNumber (was offset) • threat-hunting/counts removed input parameter: offset • threat-hunting/set-query-state removed input parameter: scheduled
March 2023	Version 5.0.3 SP1

About This Guide

This document describes the Fortinet Endpoint Protection and Response Platform (FortiEDR) RESTful API and its usage. It is intended for the following types of users:

- **Security Engineers/Administrators,** who are responsible for the entire Fortinet Endpoint Protection and Response Platform system, including installing, configuring, tuning and monitoring its health.
- **Security Operation Center (SOC) Operators and Analysts,** who monitor and handle Fortinet Endpoint Protection and Response Platform events. Monitoring can be performed in the Fortinet Endpoint Protection and Response Platform Central Manager or in a Security Information and Event Management (SIEM) system that is fed events from the Fortinet Endpoint Protection and Response Platform.
- **Forensic Investigators,** who will perform deep, drilldown analysis and investigation of Fortinet Endpoint Protection and Response Platform events.

FortiEDR Rest APIs are also documented within the user interface of the Central Manager console. To open a brief version of this Rest API guide, use rest-ui postfix on your FortiEDR Central Manager's URL:
https://{ensilo-host}/rest-ui

Chapter 1 – FortiEDR RESTFUL API

This document describes the FortiEDR RESTful API and its usage.

Overview

FortiEDR's RESTful API enables you to easily integrate FortiEDR functionality into your organization's existing software.

The Fortinet Endpoint Protection and Response Platform Central Manager supports a REST HTTP-based API for accessing security and application communication control data, as well as device and software configuration and operations.

All the functionality described in this chapter is also available using the Central Manager Web user interface, which is described throughout this guide.

The API uses JSON as the format for both requests and responses.

Errors may be returned for each API call, as described below.

For operations involving files, the response format is a file stream (binary data).

This chapter is divided into several logical sections. Each section describes the associated REST API functionality that is supported.

The API uses Token Based Authentication for authenticating the calls, as described in the *Authorization* section on page 10.

The Central Manager is limited to using only the HTTPS protocol and therefore all traffic using the API is encrypted – both in and out.

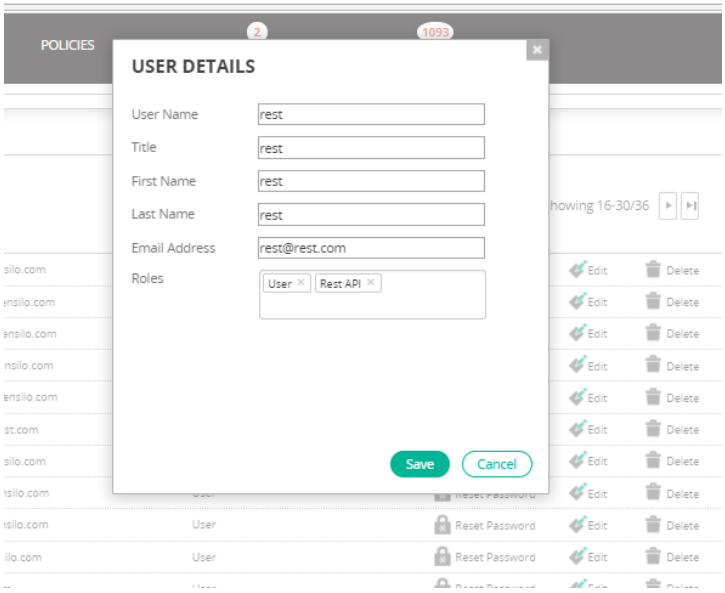
Authorization

The Fortinet Endpoint Protection and Response Platform REST API layer requires user authorization in order to perform API calls. You can use one of the following authorization methods:

- **Basic Authentication,** page 10
- **API Authorization Token,** page 11

Basic Authentication

To perform a request to the Fortinet Endpoint Protection and Response Platform REST API layer, the user performing the calls must have the relevant **REST API** role defined, as shown below:



Note – After the creation of a FortiEDR Central Manager user with a REST API role, this newly created user must log in to the Central Manager console and change their initial password before they can be used by Rest API calls.

A user attempting to perform API calls without the **REST API** role gets a **401 Unauthorized Access** error code. The Admin role does not provide access to the REST API layer, and does not contain the Rest API role.

Assigning a user the REST API role automatically generates the **X-Auth-Token** in the Fortinet Endpoint Protection and Response Platform Central Manager. Although basic authentication generates this token, the token is not required for basic authentication. The **X-Auth-Token** is required for API token authorization, as described on page 11.

After the REST API role is assigned to a user, that user can perform API calls using basic authentication by supplying only his/her user name and password. When using basic authentication, the user name and password must be supplied for each API call.

Authentication in Multi-tenancy Environments

In a multi-tenancy environment, the organization must be used as a prefix to the API user name in order to enable authentication. For example: MYORG\myuser.

API Authorization Token

Instead of basic authentication, the API authorization token method can be used to perform API calls. When using this authorization method, an authorization token must be supplied each time an API request is made, in lieu of supplying the user's user name and password. Page 10 describes how to obtain an **X-Auth-Token**.

Basic authentication must be used at least once, in order to obtain the token required for API token authorization. The **X-Auth-Token** authorization token must be supplied each time an API request is made via the HTTP **"X-Auth-Token" request header**.

You may periodically want to generate a new authentication token. To do so, a new request to the API layer is required that uses basic authentication. This generates a new token, as described on page 10, which revokes the previous authentication token.

Authentication tokens are valid for the duration of the TCP session, which expires after 60 seconds of inactivity. To establish a new connection, re-authenticate and generate a new "X-Auth-Token". Note that tokens have a maximum lifespan of 4 hours, regardless of the TCP session state.

Example

To use the API authentication token for API calls:

1. Configure a FortiEDR user with a Rest API role, as described in the Basic Authentication section on page 10.
2. Encode the user and password in base64: `echo -n "org\user:password" | base64.` For example: echo -n "Fortinet Demo - EMEA\user123:password123" | base64
3. Issue an API using the encoded user and password, as follows:
   ```
   curl -i -H "Authorization:Basic dXNlcjpwYXNzd29yZA==" https://ENSILOHOST/management-rest/events/list-events -I
   ```
4. The "**X-Auth-Token**" header is received in the **response headers**. For example:
   ```
   HTTP/1.1 200
   Set-Cookie: JSESSIONID=19D788C715E08598E4DA3A398DCC619D; Path=/; Secure; HttpOnly; SameSite=None
   X-Auth-Token: nyujIopt1Kzlk1Aajwmb6huIVdG/8mRyUpB72+sagEQ=
   Content-Type: application/json
   Transfer-Encoding: chunked
   Date: Thu, 29 Apr 2021 21:33:08 GMT
   ```
5. This **X-Auth-Token** can now be used, instead of providing user name and password credentials. For example:
   ```
   curl -k -H "X-Auth-Token: nyujIopt1Kzlk1Aajwmb6huIVdG/8mRyUpB72+sagEQ="
   https://ENSILOHOST/management-rest/events/list-events
   ```

If there is an unauthorized access attempt to the REST API layer, a **"401 Unauthorized Access"** error code is returned.

Request Format and Special Characters

Two parameter types are passed in the REST API calls: URL parameters and Body parameters. Each type is described below.

URL Parameters

URL parameters are used for search purposes.

A comma-separated list is used when dealing with multiple values for the same search field.

Example:

GET

https://ENSILOHOST/management-rest/events/list-events?eventIds=1000,1001,1002

Passing a **comma** inside a search parameter value is possible using a backslash (\) as an escape character, as shown below:

https:// ENSILOHOST/management-rest/comm-control/list-products?versions=1\,1\,1

The example above means the list of all vendors having a child version **1,1,1**.

Body Parameters

Body parameters are used to update or create and are supplied in JSON format in the request body.

Example:

PUT

https://ENSILORHOST/management-rest/events/eventIds=1000,1001,1002

Request Body:

```
{
    "read": true
}
```

Events

list-events (GET)

This API call outputs all the events in the system that match the condition(s) you specify in the call. An AND relationship exists when specifying multiple input parameters. When no input parameters are matched, an empty result set is returned:

- **Input Parameters –** Can be any combination of the following parameters in order to query for data:
  - **eventIds:** Specifies the required event IDs. Number format.
  - **device:** Specifies the device name where the events occurred.
  - **collectorGroups:** Specifies the collector groups whose collector reported the events.
  - **operatingSystems:** Specifies the operating system of the devices where the events occurred.
  - **deviceIps:** Specifies the IPs of the devices where the event occurred.
  - **macAddresses:** Specifies the MAC addresses where the event occurred.
  - **fileHash:** Specifies the hash signature of the main process of the event.
  - **process:** Specifies the main process of the event.
  - **paths:** Specifies the paths of the processes related to the event.
  - **firstSeen:** Specifies the date when the event was first seen.

    Date Format: yyyy-MM-dd HH:mm:ss (Deprecated).
  - **lastSeen:** Specifies the date when the event was last seen.

    Date Format: yyyy-MM-dd HH:mm:ss (Deprecated).
  - **firstSeenFrom:** Specifies the “from” date when the event was first seen. Use this parameter together with the **firstSeenTo** parameter to specify a date range.

    Date Format: yyyy-MM-dd HH:mm:ss.
  - **firstSeenTo:** Specifies the “to” date when the event was first seen. Use this parameter together with the **firstSeenFrom** parameter to specify a date range.

    Date Format: yyyy-MM-dd HH:mm:ss.
  - **lastSeenFrom:** Specifies the “from date” when the event was last seen. Use this parameter together with the **lastSeenTo** parameter to specify a date range.

    Date Format: yyyy-MM-dd HH:mm:ss.
  - **lastSeenTo:** Specifies the “to” date when the event was last seen. Use this parameter together with the **lastSeenFrom** parameter to specify a date range.

    Date Format: yyyy-MM-dd HH:mm:ss.
  - **seen:** A true/false parameter indicating whether events were read/unread by the user operating the API.
  - **handled:** A true/false parameter indicating whether events were handled/unhandled.
  - **severities:** A string with one of the following values: Critical, High or Medium.
  - **classifications:** A list of strings with one of the following values: Malicious, Suspicious, Inconclusive, Likely Safe, PUP or Safe (from version: Citroën).
  - **destinations:** Specifies the connection destination(s) of the events.
  - **actions:** A string with one of the following values: Block, SimulationBlock or Log.
  - **rule:** Specifies the short rule name of the rule that triggered the events.
  - **archived:** A true/false parameter indicating whether to include only archived events.
  - **signed:** A true/false parameter indicating whether the event is signed.
  - **loggedUser:** Specifies the logged-in user.
  - **strictMode:** A true/false parameter indicating whether or not to perform strict matching on the search parameters. The default is False.
  - **pageNumber:** An integer used for paging that indicates the required page number.
  - **itemsPerPage:** An integer used for paging that indicates the number of events to retrieve for the current page. The default is 100. The maximum value is 2,000.

- **sorting:** Specifies a list of strings in JSON format representing the fields by which to sort the results in the following format: "column1":true, "column2":false.
  True indicates to sort in descending order. Results are sorted by the first field, then by the second field and so on.
- **muted:** A true/false parameter indicating whether the event is muted.
- **deviceControl:** A true/false parameter indicating whether to only include device control events.
- **expired:** A true/false parameter indicating whether to only include expired events.
- **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
  - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
  - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.

- **Output Parameters –** For each event that matches the query, the following parameters are exported:
  - **eventId**: Specifies the ID of the event.
  - **collectors:** Specifies the list of the collectors that reported this event with the following fields:
    - **device:** Specifies the device name.
    - **collectorGroup:** Specifies the name of the collector group to which the collector belongs.
    - **deviceIp:** Specifies the IP of the device.
    - **os:** Specifies the operating system of the device.
    - **collectorLastSeen:** Specifies the date when the collector was last seen.
  - **process:** Specifies the name of the main process of the event.
  - **processType:** Specifies the process type, which can be 32 bit or 64 bit.
  - **certified:** Indicates whether the main process is signed.
  - **processPath:** Specifies the path of the main process.
  - **severity:** Indicates the severity, which can be Critical, High or Medium (Deprecated).
  - **seen:** A true/false parameter indicating whether events were read/unread by the user operating the API.
  - **destinations:** Specifies the list of all the communication destination(s) (IP format) that are relevant for this event.
  - **firstSeen:** Specifies the date when this event was first seen.
  - **lastSeen:** Specifies the date when this event was last seen.
  - **action:** A string with one of the following values: Block, SimulationBlock or Log.
  - **handled:** Indicates whether the event was handled.
  - **comment:** Specifies a user-defined string to attach to the exception.
  - **archived:** A true/false parameter indicating whether to include archived events.
  - **classification:** A string with one of the following values: Malicious, Suspicious, Inconclusive, Likely Safe, PUP or Safe.
  - **rules:** Specifies list of the short rule name of the rules that triggered the events.
  - **threatDetails** (supported for version 5.0.3.334 and above)**:** Specifies the following threat details if threat intelligence data is available for the threat.
    - **threatFamily:** Specifies the family of the threat.
    - **threatType:** Specifies the type of the threat.
    - **threatName:** Specifies the name of the threat.
  - **loggedUsers:** Specifies list of the logged-in users.
  - **muted:** A true/false parameter indicating whether the event is muted.
  - **muteEndTime:** Indicates the mute end time.
  - **processOwner**: Indicates the process owner.

- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.
  - Error code 400 is returned if **firstSeen** is later than the current date.
  - Error code 400 is returned if **firstSeen** is later than **lastSeen**.

Sample Request

https://ENSILORHOST/management-rest/events/list-events?eventIds=1000,1001&device=myDevice&collectorGroups=Default Collector Group,Servers&deviceIps=1.2.3.4,5.6.7.8&severities=Critical,High&actions=Block,SimulationBlock&paths=\device0\Users,\device0\Documents&process=explorer.exe&fileHash=ADF34CKD83682HBJDF82G3&firstSeen=2016-05-01 00:00:00&lastSeen=2016-05-31 00:00:00&seen=false&handled=false&destinations=100.100.100.100&rule=Fake Critical Program&sorting="lastSeen":true

Sample Response


```
{
    "eventId": 1000,
    "collectors": [
      {
        "lastSeen": "2016-06-19 17:15",
        "os": "Windows 10 Home",
        "deviceIp": "192.168.1.3",
        "device": "myDevice"
        "collectorGroup": "Default Collector Group"
      },
      {
        "lastSeen": "2016-06-19 17:15",
        "os": "Windows 10 Home",
        " deviceIp ": "10.0.0.10",
        "device": "myDevice2",
        "collectorGroup": "Default Collector Group"
      } ]
    "process": "explorer.exe",
    "processPath": "\\Device0\\Users",
    "processType": "64bit",
    "firstSeen": "31-May-2016, 11:57:36",
    "lastSeen": "31-May-2016, 12:02:55",
    "read": false,
    "handled": false,
    "certified": false,
    "severity": "Critical",
    "destination": "100.100.100.100",
    "action": "Block"
  }
```

list-raw-data-items (GET)

This API call outputs the raw data items for an event ID. The event ID is mandatory. All other input parameters except the event ID are optional. If no input parameters are specified, an empty result set is returned:

- **Input Parameters –** Can be any combination of these parameters in order to query for data:
  - **eventId:** Specifies the ID of the event that holds the raw data items. This parameter is mandatory.
  - **device:** Specifies the name of the device where the raw event occurred.
  - **collectorGroups:** Specifies the collector groups whose collector reported the raw events.
  - **firstSeen:** Specifies the date when the event was first seen.

    Date Format: yyyy-MM-dd HH:mm:ss (Deprecated).
  - **lastSeen:** Specifies the date when the event was last seen.

    Date Format: yyyy-MM-dd HH:mm:ss (Deprecated).
  - **firstSeenFrom:** Specifies the “from” date when the event was first seen. Use this parameter together with the **firstSeenTo** parameter to specify a date range.

    Date Format: yyyy-MM-dd HH:mm:ss.
  - **firstSeenTo:** Specifies the “to” date when the event was first seen. Use this parameter together with the **firstSeenFrom** parameter to specify a date range.

    Date Format: yyyy-MM-dd HH:mm:ss.
  - **lastSeenFrom:** Specifies the “from” date when the event was last seen. Use this parameter together with the **lastSeenTo** parameter to specify a date range.

    Date Format: yyyy-MM-dd HH:mm:ss.
  - **lastSeenTo:** Specifies the “to” date when the event was last seen. Use this parameter together with the **lastSeenFrom** parameter to specify a date range.

    Date Format: yyyy-MM-dd HH:mm:ss.
  - **strictMode:** A true/false parameter indicating whether to perform strict matching on the search parameters. The default is False.
  - **rawEventIds:** Specifies the list of raw data item event IDs.
  - **pageNumber:** An integer used for paging that indicates the required page number.
  - **itemsPerPage:** An integer used for paging that indicates the number of events to retrieve for the current page. The default is 100. The maximum value is 2,000.
  - **sorting:** Specifies a list of strings in JSON format representing the fields by which to sort the results in the following format: `"column1":true, "column2":false.`

    True indicates to sort in descending order. Results are sorted by the first field, then by the second field and so on.
  - **fullDataRequested:** A true/false parameter indicating whether to include the event internal information.
- **Output Parameters –** For each event that matches the query, the following parameters are exported:
  - **eventId:** Specifies the ID of the event that holds the raw data item.
  - **rawEventId:** Specifies the ID of the raw data item.
  - **device:** Specifies the name of the device where the raw event occurred.
  - **deviceIp:** Specifies the IP of the device where the raw event occurred.
  - **destinations:** Specifies the communication destination(s) (IP format).
  - **firstSeen:** Specifies the date when the raw data item was first seen.

    Date Format: yyyy-MM-dd HH:mm:ss.
  - **lastSeen:** Specifies the date when the raw data items was last seen.

    Date Format: yyyy-MM-dd HH:mm:ss.
  - **count:** Specifies the number of exact raw data items that matched this raw data item.
  - **remediateDevice** (supported for version 5.0.3.334 and above)**:** Specifies the details of the recommended remediation.
    - **executablesToRemove:** Provides a list of files that are associated with the event.
    - **ProcessesToTerminate:** Provides a list of processes that are associated with the event.

    - **PersistenceDataAction:** Provides a list of registry keys that are associated with the event.
- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.
  - Error code 400 is returned if **firstSeen** is later than the current date.
  - Error code 400 is returned if **firstSeen** is later than **lastSeen**.

Sample Request

https://ENSILOHOST/management-rest/events/list-raw-data-items?eventId=1000&rawEventIds=123456789,234567890&device=myDevice&collectorGroups=Default Collector Group,Servers&deviceIps=1.2.3.4,5.6.7.8&process=explorer.exe&firstSeen=2016-05-01 00:00:00&lastSeen=2016-05-31 00:00:00 &destinations=100.100.100.100&&sorting="lastSeen":
true

Sample Response


```
[
 {
    "eventId": 146910,
    "rawEventId": 98088525,
    "device": "HOME-PC1",
    "deviceIp": "10.0.0.1",
    "destination": "142.4.219.38",
    "firstSeen": "30-May-2016 20:03:19",
    "lastSeen": "30-May-2016 20:03:19",
    "count": 1
  },
 {
    "eventId": 146910,
    "rawEventId": 98088519,
    "device": "HOME-PC1",
    "deviceIp": "10.0.0.2",
    "destination": "151.80.33.144",
    "firstSeen": "30-May-2016 20:03:18",
    "lastSeen": "30-May-2016 20:03:18",
    "count": 1
  }
]
```


Update Events (PUT)

This API call updates the read/unread, handled/unhandled or archived/unarchived state of an event. The output of this call is a message indicating whether the update succeeded or failed:

- **Input Parameters –** Can be any combination of these parameters in order to query for data:
  - **eventIds:** Specifies the required event IDs. Number format.

    Note – For an event that occurs on multiple devices, updates affect all of these devices.
  - **device:** Specifies the device name where the events occurred.
  - **collectorGroups:** Specifies the collector groups whose collector reported the events.
  - **operatingSystems:** Specifies the operating system of the devices where the events occurred.
  - **deviceIps:** Specifies the IPs of the devices where the event occurred.
  - **fileHash:** Specifies the hash signature of the main process of the event.

- **process:** Specifies the main process of the event.
- **paths:** Specifies the processes related to the event.
- **firstSeen:** Specifies the date when the event was first seen.

  Date Format: yyyy-MM-dd HH:mm:ss (Deprecated).
- **lastSeen:** Specifies the date when the event was last seen.

  Date Format: yyyy-MM-dd HH:mm:ss (Deprecated).
- **firstSeenFrom:** Specifies the “from” date when the event was first seen. Use this parameter together with the **firstSeenTo** parameter to specify a date range.

  Date Format: yyyy-MM-dd HH:mm:ss.
- **firstSeenTo:** Specifies the “to” date when the event was first seen. Use this parameter together with the **firstSeenFrom** parameter to specify a date range.

  Date Format: yyyy-MM-dd HH:mm:ss.
- **lastSeenFrom:** Specifies the “from” date when the event was last seen. Use this parameter together with the **lastSeenTo** parameter to specify a date range.

  Date Format: yyyy-MM-dd HH:mm:ss.
- **lastSeenTo:** Specifies the “to” date when the event was last seen. Use this parameter together with the **lastSeenFrom** parameter to specify a date range.

  Date Format: yyyy-MM-dd HH:mm:ss.
- **seen:** A true/false parameter indicating whether the events were read/unread by the user operating the API.
- **handled:** A true/false parameter indicating whether the events were handled/unhandled.
- **severities:** A string with one of the following values: Critical, High or Medium.
- **destinations:** Specifies the connection destination(s) of the events.
- **actions:** A string with one of the following values: Block, SimulationBlock or Log.
- **rule:** Specifies the short rule name of a rule that triggered the events.
- **strictMode:** A true/false parameter indicating whether to perform strict matching on the search parameters. The default is False.
- **classifications:** A list of strings with one of the following values: Malicious, Suspicious, Inconclusive, Likely Safe, PUP or Safe (supported in V2.7.3 and above).
- **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
  - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
  - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.
- **muted:** A true/false parameter indicating whether the event is muted.
- **deviceControl:** A true/false parameter indicating whether to only include device control events.
- **expired:** A true/false parameter indicating whether to only include expired events.

- **Body Input Parameters –** It is possible to combine a handle and a comment or a classification and a comment. However, only a single field of the following can be updated at a time: archive, read, handle.
  - **read:** A true/false parameter that marks the events as read/unread.
  - **handle:** A true/false parameter that indicates whether the events were handled/unhandled.
  - **archive:** A true/false parameter indicating whether to hide/unhide the events.
  - **comment** (supported for version 2.6.4 and above)**:** Free text to be added as a comment to the event. The event must be *handled* in order to accept comments.
  - **classification:** A string with one of the following values: Malicious, PUP or Safe (supported in V2.7.3 and above).

- **mute:** A true/false parameter indicating whether to mute events.
- **muteDuration:** Specifies the mute duration time. Allowed values are Week, Month, Year or Permanently.
- **forceUnmute:** Indicates whether to force an archive even when the event is muted.
- **familyName**: Specifies the event's family name.
- **malwareType**: Specifies the event's malware type.
- **threatName**: Specifies the event's threat name.

- **Output Parameters –** Response code 200 indicates a successful operation.
- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.
  - Error code 400 is returned if **firstSeen** is later than the current date.
  - Error code 400 is returned if **firstSeen** is later than **lastSeen**.

Sample Request

https://ENSILOHOST/management-rest/events?eventIds=1000,1001&device=myDevice&collectorGroups=Default Collector Group,Servers&

deviceIps=1.2.3.4,5.6.7.8&severities=Critical,High&actions=Block,SimulationBlock&paths=\device0\Users, \device0\Documents&process=explorer.exe&fileHash=ADF34CKD83682HBJDF82G3&firstSeen=2016-05-01 00:00:00&lastSeen=2016-05-31 00:00:00&seen=false&handled=false&destinations=100.100.100.100&rule=Fake Critical Program

Request Type: **PUT**

Request Header: Content-Type: Application/JSON

Request Body:

```
{
   "read": true,
}
```

In the sample request above, all the events that match the search criteria are marked as read, unhandled and are set as hidden.

Delete Events (DELETE)

This API call specifies the event(s) to be deleted, based on a condition(s). For example, events can be deleted based on their event ID, time range, device and so on. The output of this call is a message indicating whether the deletion succeeded or failed:

- **Input Parameters** – Can be any combination of these parameters in order to query for data:
  - **eventIds:** Specifies the required event IDs. Number format.
  - **deleteAll:** A true/false parameter. True deletes all events. When this value is set to true, no other filtering parameter(s) can be combined in the same request.
  - **device:** Specifies the device name where the events occurred.
  - **collectorGroups:** Specifies the collector groups whose collector reported the events.
  - **operatingSystems:** Specifies the operating system of the devices where the events occurred.
  - **deviceIps:** Specifies the IPs of the devices where the event occurred.
  - **macAddresses:** Specifies the MAC addresses where the event occurred.
  - **fileHash:** Specifies the hash signature of the main process of the event.
  - **process:** Specifies the main process of the event.
  - **paths:** Specifies the paths of the processes related to the event.
  - **firstSeen:** Specifies the date when the event was first seen.

Date Format: yyyy-MM-dd HH:mm:ss (Deprecated).

- **lastSeen:** Specifies the date when the event was last seen.

  Date Format: yyyy-MM-dd HH:mm:ss (Deprecated).
- **firstSeenFrom:** Specifies the “from” date when the event was first seen. Use this parameter together with the **firstSeenTo** parameter to specify a date range.

  Date Format: yyyy-MM-dd HH:mm:ss.
- **firstSeenTo:** Specifies the “to” date when the event was first seen. Use this parameter together with the **firstSeenFrom** parameter to specify a date range.

  Date Format: yyyy-MM-dd HH:mm:ss.
- **lastSeenFrom:** Specifies the “from” date when the event was last seen. Use this parameter together with the **lastSeenTo** parameter to specify a date range.

  Date Format: yyyy-MM-dd HH:mm:ss.
- **lastSeenTo:** Specifies the “to” date when the event was last seen. Use this parameter together with the **lastSeenFrom** parameter to specify a date range.

  Date Format: yyyy-MM-dd HH:mm:ss.
- **seen:** A true/false parameter indicating whether the events were read/unread by the user operating the API.
- **handled:** A true/false parameter indicating whether the events were handled/unhandled.
- **severities:** A string with one of the following values: Critical, High or Medium.
- **classifications:** A list of strings with one of the following values: Malicious, Suspicious, Inconclusive, Likely Safe, PUP or Safe (from version: Citroën).
- **destinations:** Specifies the connection destination(s) of the events.
- **actions:** A string with one of the following values: Block, SimulationBlock or Log.
- **rule:** Specifies the short rule name of a rule that triggered the events.
- **loggedUser:** Specifies the logged-in user.
- **archived:** A true/false parameter indicating whether to include archived events.
- **signed:** A true/false parameter indicating whether the event is signed.
- **pageNumber:** An integer used for paging that indicates the required page number.
- **itemsPerPage:** An integer used for paging that indicates the number of collectors to retrieve for the current page. The default is 100. The maximum value is 2,000.
- **sorting:** Specifies a list of strings in JSON format representing the fields by which to sort the results in the following format: "column1":true, "column2":false. True indicates to sort in descending order. Results are sorted by the first field, then by the second field and so on.
- **strictMode:** A true/false parameter indicating whether to perform strict matching on the search parameters. The default is False.
- **muted:** A true/false parameter indicating whether the event is muted.
- **deviceControl**: A true/false parameter indicating whether to only include device control events.
- **expired**: A true/false parameter indicating whether to only include expired events.
- **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
  - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
  - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.

- **Output Parameters –** None.

  Response code 200 indicates a successful operation.
- **Errors:**

- Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
- Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.
- Error code 400 is returned if **firstSeen** is later than the current date.
- Error code 400 is returned if **firstSeen** is later than **lastSeen**.

Sample Request

https://ENSILORHOST/management-rest/events/list-events?eventIds=1000,1001&device=myDevice&collectorGroups=Default Collector Group,Servers&deviceIps=1.2.3.4,5.6.7.8&severities=Critical,High&actions=Block,SimulationBlock&paths=\device0\Users,\device0\Documents&process=explorer.exe&fileHash=ADF34CKD83682HBJDF82G3&firstSeen=2016-05-01 00:00:00&lastSeen=2016-05-31 00:00:00&seen=false&handled=false&destinations=100.100.100.100&rule=Fake Critical Program

Request Type: **DELETE**

In the sample request above, all the events matching the search criteria are deleted.

create-exception (POST)

This API call adds an exception to a specific event. The output of this call is a message indicating whether the creation of the exception succeeded or failed:

- **Input Parameters –** Can be any combination of these parameters in order to query for data:
  - **exceptionId:** Specifies the exception ID to edit.
  - **eventId:** Specifies the event ID on which to create the exception. Number format. This parameter is mandatory.
  - **collectorGroups:** Specifies the list of all the collector groups to which the exception should be applied. When not used, all collector groups are selected.
  - **allCollectorGroups:** A true/false parameter indicating whether the exception should be applied to all collector groups. When not used, all collector groups are selected.
  - **allOrganizations:** A true/false parameter indicating whether the exception should be applied to all organizations (tenants). This parameter is only relevant in a multi-tenancy environment. This parameter is only allowed for users with hoster privileges (general administrator).
  - **destinations:** A list of IPs to which the exception applies and/or the value *internal destinations*.
  - **allDestinations:** A true/false parameter indicating whether the exception should be applied to all destinations. When not used, all destinations are selected.
  - **users:** A list of users to which the exception should be applied.
  - **allUsers:** A true/false parameter indicating whether the exception should be applied to all users. When not used, all users are selected.
  - **comment** (supported for version 2.6.4 and above)**:** Specifies a user-defined string to attach to the exception.
  - **forceCreate:** A true/false parameter indicating whether to create the exception, even if there are already exceptions that cover this given event.
- **Body Input Parameters** (optional; supported for version 2.6.4 and above): If not used, default settings are applied.

  In order to set the advanced settings of an exception, the user must know which processes exist in the event and which rules were triggered:
  - **useInException:** For each relevant process in each relevant rule, the user must indicate true/false in order to include it in the exception.
  - **useAnyPath:** For each relevant process in each relevant rule, the user must indicate true/false to set an exception on the path that was seen in the event or for any path.
  - **wildcardFiles** (supported for Dodge EN-9330 version and above)**:** For each relevant process in each relevant rule file name, checks whether the pattern matches the file value, and according to the action (true/false), attaches/removes the exception wildcard field.

- **wildcardPaths** (supported for Dodge EN-9330 version and above)**:** For each relevant process in each relevant rule path name, checks whether the pattern matches the file value, and according to the action (true/false), attaches/removes the exception wildcard field.

- **Output Parameters –** None.

  Response code 200 indicates a successful operation.

- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

Sample Request

https:// ENSILOHOST/management-rest/events/create-exception?eventId=1000&allCollectorGroups=false&collectorGroups=OSX Users,Home Users&allDestinations=false&destinations=1.2.3.4,5.6.7.8,internal destinations,forceCreate=true

Request Type: **POST**

Request Body:

```
{
   "useInException" : {
         " dynamicCode.exe " : {
               "Unmapped Executable" : true,
               "Executable Format": true,
               "Dynamic Code" : false,
               "Writeable Code" : false
         },
         " dynamic.dll" : {
               "Unmapped Executable" : false
         }
   },
   "useAnyPath" : {
         " dynamicCode.exe " : {
               "Dynamic Code" : true,
               "Executable Format": false,
               "Unmapped Executable" : true,
               "Writeable Code" : true
         },

         " dynamic.dll": {
               "Unmapped Executable" : true
         }
   }
}
```

count-events (GET)

This API call counts events. This API call is supported for version 3.1 and above:

- **Input Parameters:**
  - **eventIds:** Specifies the required event IDs in numeric format.
  - **device:** Specifies the device name where the event occurred.
  - **collectorGroups:** Specifies the collector groups whose collector reported the event.
  - **operatingSystems:** Specifies the operating system of the devices where the event occurred.
  - **deviceIps:** Specifies the IPs of the devices where the event occurred.
  - **macAddresses:** Specifies the MAC addresses where the event occurred.
  - **fileHash:** Specifies the hash signature of the main process of the event.
  - **process:** Specifies the main process of the event.
  - **paths:** Specifies the paths of the processes related to the event.
  - **firstSeen:** Specifies the date when the event was first seen.

    Date Format: yyyy-MM-dd HH:mm:ss (Deprecated).
  - **lastSeen:** Specifies the date when the event was last seen.

    Date Format: yyyy-MM-dd HH:mm:ss (Deprecated).
  - **firstSeenFrom:** Specifies the “from” date when the event was first seen. Use this parameter together with the **firstSeenTo** parameter to specify a date range.

    Date Format: yyyy-MM-dd HH:mm:ss.
  - **firstSeenTo:** Specifies the “to” date when the event was first seen. Use this parameter together with the **firstSeenFrom** parameter to specify a date range.

    Date Format: yyyy-MM-dd HH:mm:ss.
  - **lastSeenFrom:** Specifies the “from” date when the event was last seen. Use this parameter together with the **lastSeenTo** parameter to specify a date range.

    Date Format: yyyy-MM-dd HH:mm:ss.
  - **lastSeenTo:** Specifies the “to” date when the event was last seen. Use this parameter together with the **lastSeenFrom** parameter to specify a date range.

    Date Format: yyyy-MM-dd HH:mm:ss.
  - **seen:** A true/false parameter indicating whether events were read/unread by the user operating the API.
  - **handled:** A true/false parameter indicating whether events were handled/unhandled.
  - **severities:** A string with one of the following values: Critical, High or Medium.
  - **classifications:** A list of strings with one of the following values: Malicious, Suspicious, Inconclusive, Likely Safe, PUP, Safe (from version: Citroën).
  - **destinations:** Specifies the connection destination(s) of the events.
  - **actions:** A string with one of the following values: Block, SimulationBlock or Log.
  - **rule:** Specifies the short rule name of the rule that triggered the event.
  - **archived:** A true/false parameter indicating whether to only include archived events.
  - **signed:** A true/false parameter indicating whether the event is signed.
  - **loggedUser:** Specifies the logged-in user.
  - **strictMode:** A true/false parameter indicating whether or not to perform strict matching on the search parameters. The default is False.
  - **muted:** A true/false parameter indicating whether the event is muted.
  - **deviceControl**: A true/false parameter indicating whether to only include device control events.
  - **expired**: A true/false parameter indicating whether to only include expired events.
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:

  - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
  - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.

    Results are sorted by the first field, then by the second field and so on.
- **Output:** Outputs a count of the number of events that match the specified search criteria.

export-raw-data-items-json

This API call exports raw data item events in JSON format.

- **Input Parameters:**
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **rawItemIds:** Specifies the raw data item event IDs.
- **Output Parameters:** This operation results in a file stream (binary data), which is a *.zip file.

Sample Request

https:// ENSILOHOST/management-rest/events/export-raw-data-items-json?rawItemIds=1234&organization=test

Exceptions

get-event-exceptions (GET)

This API call shows all exceptions for an event:

- **Input Parameters:**
  - **eventId:** Specifies the required event ID. This parameter is mandatory.
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
- **Output Parameters –** Provides a list of exceptions:
  - **exceptionId:** Specifies the exception ID.
  - **originEventId:** Specifies the event ID.
  - **userName:** Specifies the user who created the exception.
  - **createdAt:** Specifies when the exception was created.
  - **updatedAt:** Specifies when the exception was last updated.
  - **comment:** Specifies a user-defined string attached to the exception.
  - **selectedDestination:** Specifies the list of selected destinations.
  - **optionalDestinations:** Specifies the list of destinations not selected.
  - **selectedCollectorGroups:** Specifies the list of selected collector groups.
  - **optionalCollectorGroups:** Specifies the list of unselected collector groups.
  - **optionalUsers:** Specifies the list of users that are not included in the exception.
  - **selectedUsers**: Specifies the list of users that are included in the exception.
  - **organization:** Specifies the organization of the exception.
  - **alerts:** Specifies the list of alerts. Each alert has the following parameters:
    - **ruleName:** Specifies the rule name.
    - **process:** Specifies the first process that is part of the exception.
    - **process2:** Specifies the second process that is part of the exception.
    - **script:** Specifies the script for the first process.
    - **process2Script:** Specifies the script for the second process.

    The **process**, **process2, script** and **process2Script** fields each contain the following fields:
    - **name:** Specifies the process name.
    - **path:** Specifies the process path.
    - **usedInException:** A true/false parameter indicating whether the process is used by the exception in advanced configuration.
    - **useAnyPath:** A true/false parameter indicating whether the process is used by the exception in advanced configuration.
    - **signed:** A true/false parameter indicating whether the process is signed.
- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

Sample Request

https:// ENSILOHOST/management-rest/exceptions/get-event-exceptions?eventId=538022

Sample Response


```
[
   {
      "exceptionId": 633627,
"originEventId": 538022,
```

```
"userName": "admin",
"updatedAt": "2017-12-03 12:18",
"comment": null,
"selectedDestinations": [
"All Destinations"
      ],
      "optionalDestinations": [
      "All Internal destinations",
      "74.125.235.20"
      ],
      "selectedCollectorGroups": [
      "All Collector Groups"
      ],
      "optionalCollectorGroups": [
      "group1",
      "group2"
      ],
      "alerts": [
   {
      "ruleName": "Stack Tampering",
      "process": {
      "name": "EvilProcessTests.exe",
      "path": "\\Users\\root\\Desktop\\malwareSimulation",
      "usedInException": true,
      "useAnyPath": true,
      "signed": true
            }
      }
            ]
      }
   ]
```


Delete (DELETE)

This API call deletes an exception:

- **Input Parameters:**
  - **exceptionId:** Specifies the required exception ID. This parameter is mandatory.
  - **exceptionIds:** Specifies a list of exception IDs.
  - **collectorGroups:** Specifies the list of all the collector groups to which the exception applied.
  - **createdBefore:** Specifies the date before which the exception was created. Specify the date using the yyyy-MM-dd HH:mm:ss format.
  - **createdAfter:** Specifies the date after which the exception was created. Specify the date using the yyyy-MM-dd HH:mm:ss format.
  - **updatedBefore:** Specifies the date before which the exception was updated. Specify the date using the yyyy-MM-dd HH:mm:ss format.
  - **updatedAfter:** Specifies the date after which the exception was updated. Specify the date using the yyyy-MM-dd HH:mm:ss format.
  - **process:** Specifies the process of the exception.
  - **path:** Specifies the path of the exception.
  - **comment:** Specifies a comment that is attached to the exception.
  - **destination:** Specifies a destination IP of the exception.

- **user:** Specifies a user of the exception.
- **deleteAll:** A true/false parameter indicating whether all the exceptions should be deleted.
- **rules:** Specifies a list of rule names.
- **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.

- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

Sample Request

https:// ENSILOHOST/management-rest/exceptions/delete?exceptionId=538022

list-exceptions (GET)

This API call outputs a list of exceptions (supported in V2.7.3 and above):

- **Input Parameters:**
  - **createdBefore:** Specifies the date before which the exception was created. Specify the date using the yyyy-MM-dd HH:mm:ss format.
  - **createdAfter:** Specifies the date after which the exception was created. Specify the date using the yyyy-MM-dd HH:mm:ss format.
  - **updatedBefore:** Specifies the date before which the exception was updated. Specify the date using the yyyy-MM-dd HH:mm:ss format.
  - **updatedAfter:** Specifies the date after which the exception was updated. Specify the date using the yyyy-MM-dd HH:mm:ss format.
  - **exceptionIds:** Specifies a list of exception IDs.
  - **rules**: Specifies a list of rule names.
  - **collectorGroups:** Specifies the list of all the collector groups to which the exception applies.
  - **process:** Specifies the process of the exception.
  - **path:** Specifies the path of the exception.
  - **comment:** Specifies a comment attached to the exception.
  - **destination:** Specifies a destination IP of the exception.
  - **user:** Specifies a user of the exception.
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.
- **Output Parameters:**
  - **exceptionId:** Specifies the exception ID.
  - **originEventId:** Specifies the event ID.
  - **userName:** Specifies the user who created the exception.
  - **createdAt:** Specifies when the exception was created.
  - **updatedAt:** Specifies when the exception was last updated.
  - **comment:** Specifies a user-defined string attached to the exception.
  - **selectedDestination:** Specifies the list of selected destinations.
  - **optionalDestinations:** Specifies the list of unselected destinations.

- **selectedCollectorGroups:** Specifies the list of selected collector groups.
- **optionalCollectorGroups:** Specifies the list of unselected collector groups.
- **optionalUsers:** Specifies the list of users that are not selected to be included in the exception.
- **selectedUsers**: Specifies the list of users that are selected to be included in the exception.
- **organization:** Specifies the organization of the exception.
- **alerts:** Specifies the list of alerts. Each alert holds the following parameters:
  - **ruleName:** Specifies the rule name.
  - **process:** Specifies the first process that is part of the exception.
  - **process2:** Specifies a second process that is part of the exception (relevant only to some exceptions).
  - **script:** Specifies the script for the first process (relevant only to some exceptions).
  - **process2Script:** Specifies the script for the second process (relevant only to some exceptions).

    The fields **process**, **process2, script** and **process2Script** contain the following fields:
  - **name:** Specifies the process name.
  - **path:** Specifies the process path.
  - **usedInException:** A true/false field indicating whether the process is used by the exception in advanced configuration.
  - **useAnyPath:** A true/false field indicating whether the process is used by the exception in advanced configuration.
  - **signed:** A true/false field indicating whether the process is signed.
- **Errors:**
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

Sample Request

https://ENSILOHOST/management-rest/exceptions/list-exceptions

Sample Response


```
      [
{
            "exceptionId": 633627,
            "originEventId": 538022,
            "userName": "admin",
            "updatedAt": "2017-12-06 17:16",
            "comment": "\r\n--------------------------------------------\r\nadmin,
            06-Dec-2017, 17:16:02:\r\ncomment",
            "selectedDestinations":
               [
                  "All Destinations"
               ],
            "optionalDestinations":
               [
                  "All Internal destinations",
                  "74.125.235.20"
               ],
            "selectedCollectorGroups":
               [
                  "All Collector Groups"
               ],
            "optionalCollectorGroups":
               [
                  "group1",
                  "group2",
                  "All Organizations"
               ],
            "alerts":
```

```
                [
                    {
                        "ruleName": "Stack Tampering",
                        "process": {
                        "name": "EvilProcessTests.exe",
                        "path": "\\Users\\root\\Desktop\\malwareSimulation",
                        "usedInException": true,
                        "useAnyPath": true,
                        "signed": true
                    }
                }
            ]
}
      ]
```


create-or-edit-exception

This API call creates a new exception or updates an existing exception based on the given exception JSON body parameter.

- **Input Parameters:**
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
  - **confirmEdit:** Confirms the editing of an existing exception when providing an exception ID in the body JSON. By default, **confirmEdit** is false.
- **Body Parameter:**
  - **exception json:** Is retrieved by exporting an event from the management. When you export an event (with an exception), the exception JSON contains the **ExceptionId** field.
- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

Sample Request

https://ENSILOHOST/management-rest/exceptions/create-or-edit-exception?organization=orgA&confirmEdit=true

Communication Control

Fortinet's Communication Control module is responsible for monitoring and handling non-disguised security events. The module uses a set of policies that contain recommendations about whether an application should be approved or denied from communicating outside your organization.

list-products (GET)

This API call outputs a list of all the communicating applications in the system, and information about each of them:

- **Input Parameters –** Can be any combination of these parameters in order to query for data:
  - **vendors:** Specifies the list of vendor names. Names must match exactly. **strictMode** is always true.
  - **products:** Specifies the list of product names. Names must match exactly. **strictMode** is always true.
  - **versions:** Specifies the list of versions. Names must match exactly. **strictMode** is always true.
  - **vendor:** Specifies a single value for the vendor name. By default, **strictMode** is false.
  - **product:** Specifies a single value for the product name. By default, **strictMode** is false.
  - **version:** Specifies a single value for the version name. By default, **strictMode** is false.
  - **processes:** Specifies the list of process names running alongside the products.
  - **lastConnectionTimeStart:** Retrieves products whose last connection time is greater than the value assigned to this date.

    Date Format: yyyy-MM-dd HH:mm:ss.
  - **lastConnectionTimeEnd:** Retrieves products whose last connection time is less than the value assigned to this date.

    Date Format: yyyy-MM-dd HH:mm:ss.
  - **devices:** Specifies the list of device names where the products were seen.
  - **ips:** Specifies the list of IPs where the products were seen.
  - **os:** Specifies the list of operating system families where the products were seen.

    Possible Values: Windows, Windows Server and OS X.
  - **policies:** Specifies the list of policy names whose products have a specific decision, as specified in the **action** parameter. This parameter is irrelevant without b parameter (see below).
  - **action:** Indicates the action: Allow/Deny. This parameter is irrelevant without **policies** parameter (see above).
  - **strictMode:** A true/false parameter indicating whether to perform strict matching on the search parameters. The default is False.
  - **pageNumber:** An integer used for paging that indicates the required page number.
  - **itemsPerPage:** An integer, used for paging that indicates the number of **vendors** to retrieve for the current page. The default is 100. The maximum value is 2,000.
  - **collectorGroups:** Specifies the list of collector groups where the products were seen.
  - **handled:** A true/false parameter indicating whether events were handled/unhandled.
  - **processHash:** Specifies the process hash name.
  - **reputation:** Specifies the recommendation of the application: Unknown, Known Bad, Assumed Bad, Contradiction, Assumed Good or Known Good.
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
  - **vulnerabilities:** Retrieves products that are known to have the specified vulnerabilities.
  - **firstConnectionTimeStart:** Retrieves products whose first connection time is greater than the value assigned to this date.
  - **firstConnectionTimeEnd:** Retrieves products whose first connection time is less than the value assigned to this date.
  - **rulePolicy:** Specifies the policy name under which products have matched a specific rule, which is specified in the **rule** parameter.
  - **rule:** Indicates the rule. For this parameter, you must also specify the **rulePolicy** parameter.

  - **cveIdentifier:** Specifies the CVE identifier that is known to exist in the product and version. The format for this field is as follows: CVE-yyyy-nnnn.
  - **destinationIps:** Specifies list of destination IP addresses with which the product communicates.
- **Output Parameters:**
  - **vendor:** Specifies the name of the vendor.
  - **product:** Specifies the name of the product.
  - **version:** Specifies the name of the version.
  - **processes:** Specifies the list of process names running alongside the products.
  - **firstConnectionTime:** Specifies the date when the product was first seen communicating.

    Date Format: yyyy-MM-dd HH:mm:ss.
  - **lastConnectionTime:** Specifies the date when the product was last seen communicating.

    Date Format: yyyy-MM-dd HH:mm:ss.
  - **collectors:** Specifies the list of collectors that reported the product, in JSON format.

    Each collector holds the following parameters:
    - **device:** Specifies the device name.
    - **ip:** Specifies the device IP address.
    - **os:** Specifies the device operating system. Possible values are Windows, Windows Server, Linux Server and OS X.
    - **lastSeen:** Specifies the date when the collector was last seen.
  - **decisions:** Specifies the list communication control policies and their decisions for this specific product.
  - **collectorGroup:** Specifies the name of the collector group to which the collector belongs.
  - **seen:** A true/false parameter indicating whether events were read/unread by the user operating the API.
  - **handled:** A true/false parameter indicating whether events were handled/unhandled.
  - **recommendation:** Specifies the recommendation of the application: Unknown, Known Bad, Assumed Bad, Contradiction, Assumed Good or Known Good.
  - **decisionv2:** Specifies the list of communication control policies and their decisions and mode for this specific product. The following fields display:
    - **policyName:** Specifies the policy name.
    - **PolicyMode:** Specifies the policy mode.
    - **decision:** Indicates the action.
  - **organization:** The organization of the application.
  - **cves:** Specifies the list of known CVEs for the product and version.
  - **severity:** The worst CVE severity for the product and version, either: Unknown, Low, Medium, High or Critical.
- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.
  - Error code 400 is returned if **lastConnectionTimeStart** is later than the current date.
  - Error code 400 is returned if **lastConnectionTimeStart** is later than **lastConnectionTimeEnd**.

Sample Request

https:// ENSILOHOST/management-rest/comm-control/list-products?vendors=Dropbox, Inc&products=Dropbox&versions=71.4.108&6.7.8

Sample Response


```
[
  {
    "vendor": "Dropbox, Inc. (Signed)",
    "product": "Dropbox",
    "version": "",
    "processes": null,
    "firstConnectionTime": "2019-10-03 17:29:12",
    "lastConnectionTime": "2019-10-06 12:52:35",
    "collectors": [],
    "collectorsGroup": null,
    "decisions": [
      "Default Communication Control Policy: Allow",
      "Servers Policy: Deny",
      "Isolation Policy: Deny",
      "Servers Policy clone again 123456789 123456789: Deny",
      "longggggggggggggg nameeeeeeeee veryyyyyyyyyyyy: Allow",
      "123456789 123456789 123456789 123456789 1234567890: Deny"
    ],
    "decisionv2": [
      {
        "policyName": "Servers Policy clone again 123456789 123456789",
        "decision": "Deny",
        "policyMode": "Simulation"
      },
      {
        "policyName": "123456789 123456789 123456789 123456789 1234567890",
        "decision": "Deny",
        "policyMode": "Simulation"
      },
      {
        "policyName": "Servers Policy",
        "decision": "Deny",
        "policyMode": "Simulation"
      },
      {
        "policyName": "Default Communication Control Policy",
        "decision": "Allow",
        "policyMode": "Simulation"
      },
```

```
      {
        "policyName": "Isolation Policy",
        "decision": "Deny",
        "policyMode": "Prevention"
      },
      {
        "policyName": "longggggggggggggg nameeeeeeeee veryyyyyyyyyyyy",
        "decision": "Allow",
        "policyMode": "Simulation"
      }
    ],
    "seen": true,
    "handled": false,
    "recommendation": "Assumed good",
    "organization": "Default"
  },
  {
    "vendor": "Dropbox, Inc. (Signed)",
    "product": "Dropbox",
    "version": "71.4.108",
    "processes": null,
    "firstConnectionTime": "2019-10-03 17:29:12",
    "lastConnectionTime": "2019-10-03 17:30:32",
    "collectors": [],
    "collectorsGroup": null,
    "decisions": [
      "Default Communication Control Policy: Allow",
      "Servers Policy: Deny",
      "Isolation Policy: Deny",
      "Servers Policy clone again 123456789 123456789: Deny",
      "longggggggggggggg nameeeeeeeee veryyyyyyyyyyyy: Allow",
      "123456789 123456789 123456789 123456789 1234567890: Deny"
    ],
    "decisionv2": [
      {
        "policyName": "Servers Policy clone again 123456789 123456789",
        "decision": "Deny",
        "policyMode": "Simulation"
      },
      {
```

```
        "policyName": "123456789 123456789 123456789 123456789 1234567890",
        "decision": "Deny",
        "policyMode": "Simulation"
      },
      {
        "policyName": "Servers Policy",
        "decision": "Deny",
        "policyMode": "Simulation"
      },
      {
        "policyName": "Default Communication Control Policy",
        "decision": "Allow",
        "policyMode": "Simulation"
      },
      {
        "policyName": "Isolation Policy",
        "decision": "Deny",
        "policyMode": "Prevention"
      },
      {
        "policyName": "longggggggggggggg nameeeeeeeee veryyyyyyyyyyyy",
        "decision": "Allow",
        "policyMode": "Simulation"
      }
    ],
    "seen": true,
    "handled": true,
    "recommendation": "Assumed good",
    "organization": "Default",
    "cves": [
      {
        "cveIdentifier": "CVE-2019-12171",
        "description": "Dropbox.exe (and QtWebEngineProcess.exe in the Web Helper) in
the Dropbox desktop application 71.4.108.0 store cleartext credentials in memory upon
successful login or new account creation. These are not securely freed in the running
process.",
        "published": 1562591700,
        "lastModified": null,
        "lastEcsUpdated": 1562869500,
        "aggregatedImpactScore": null,
```

```
        "impact":
"{\"BaseMetricV2\":{\"BaseScore\":4.3,\"ConfidentialityImpact\":\"PARTIAL\",\"ObtainUser
Privilege\":false,\"AvailabilityImpact\":\"NONE\",\"ObtainOtherPrivilege\":false,\"Impac
tScore\":2.9,\"Severity\":\"MEDIUM\",\"AcInsufInfo\":false,\"Authentication\":\"NONE\",\
"IntegrityImpact\":\"NONE\",\"AccessVector\":\"NETWORK\",\"AccessComplexity\":\"MEDIUM\"
,\"ExploitabilityScore\":8.6,\"UserInteraction\":true,\"ObtainAllPrivilege\":false},\"Ba
seMetricV3\":{\"BaseScore\":7.8,\"ConfidentialityImpact\":\"HIGH\",\"AvailabilityImpact\
":\"HIGH\",\"Scope\":\"UNCHANGED\",\"ImpactScore\":5.9,\"AttackComplexity\":\"LOW\",\"In
tegrityImpact\":\"HIGH\",\"PrivilegesRequired\":\"NONE\",\"ExploitabilityScore\":1.8,\"A
ttackVector\":\"LOCAL\",\"UserInteraction\":true,\"BaseSeverity\":\"HIGH\"}}"
      }
    ]
  }
]
```


set-policy-mode (PUT)

This API call sets a policy to Simulation/Prevention mode:

- **Input Parameters:**
  - **policyNames:** Specifies the list of policies.
  - **mode:** Specifies the mode: Simulation or Prevention. This parameter is mandatory.
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

Sample Request

https:// ENSILOHOST/management-rest/comm-control/set-policy-mode?policies=endpoints,servers&mode=Simulation

assign-collector-group (PUT)

This API call assigns a collector group to a policy:

- **Input Parameters:**
  - **collectorGroups:** Specifies the collector groups whose collector reported the events.
  - **policyName:** Specifies the policy name. This parameter is mandatory.
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
  - **forceAssign:** Indicates whether or not to force the assignment, even if the group is assigned to similar policies.
- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

Sample Request

https://ENSILOHOST/management-rest/comm-control/assign-collector-group?collectorGroups=group1&policyName=policy1

set-policy-permission (PUT)

This API call controls the application Allow/Deny setting:

- **Input Parameters:**
  - **vendors:** Specifies the list of vendor names. Names must match exactly. **strictMode** is always true.
  - **products:** Specifies the list of product names. Names must match exactly. **strictMode** is always true.
  - **versions:** Specifies the list of versions. Names must match exactly. **strictMode** is always true.
  - **policies:** Specifies the list of policy names.
  - **signed:** A true/false parameter indicating whether the policy is signed.
  - **applyNested:** A true/false parameter indicating whether updating is inherited.
  - **decision:** Indicates the action: Allow/Deny.
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

Sample Request

https://ENSILOHOST/management-rest/comm-control/set-policy-permission?

vendors=Microsoft,google&products=office,hangouts&

versions=13.0.0, 2.0&policies=endpoints,servers&

signed=true&applyNested=true&decision=Deny

clone-policy (POST)

This API clones a communication control policy:

- **Input Parameters:**
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
  - **sourcePolicyName:** Specifies the security policy source name (required).
  - **newPolicyName:** Specifies the security policy target name.

Sample Request

https://ENSILOHOST/management-rest/ comm-control/clone-policy

list-policies (GET)

This API call outputs a list of all the communication control policies in the system, and information about each of them:

- **Input Parameters:**
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
  - **policies:** Specifies the list of policy names.
  - **rules:** Specifies the list of rules.
  - **sources:** Specifies who created the policy. Possible values are: Fortinet, User.
  - **state:** Policy rule state. Possible values are: Enabled, Disabled.
  - **decisions:** Indicates the action. Possible values are: Allow, Deny.
  - **pageNumber:** An integer used for paging that indicates the required page number.
  - **strictMode:** A true/false parameter indicating whether to perform strict matching on the search parameters. The default is False.

- **itemsPerPage:** An integer used for paging that indicates the number of collectors to retrieve for the current page. The default is 100. The maximum value is 2,000.
- **sorting:** Specifies a list of strings in JSON format representing the fields by which to sort the results in the following format: "column1":true, "column2":false. True indicates to sort in descending order. Results are sorted by the first field, by the second field and so on.

Sample Request

https://ENSILOHOST/management-rest/ comm-control/list-policies

Sample Response


```
[
  {
    "name": "Execution Prevention",
    "operationMode": "Prevention",
    "agentGroups": [
      "High Security Collector Group",
      "Default Collector Group"
    ],
    "organization": "Default",
    "rules": [
      {
        "name": "Suspicious Script Execution - A script was executed in a suspicious
context",
        "shortName": "Suspicious Script Execution",
        "enabled": "true",
        "securityAction": "Block"
      },
      {
        "name": "Suspicious Driver Load - Attempt to load a suspicious driver",
        "shortName": "Suspicious Driver Load",
        "enabled": "true",
        "securityAction": "Block"
      },
      {
        "name": "Unconfirmed File Detected",
        "shortName": "Unconfirmed File Detected",
        "enabled": "false",
        "securityAction": "Log"
      },
      {
        "name": "Malicious File Detected",
        "shortName": "Malicious File Detected",
        "enabled": "true",
        "securityAction": "Block"
      },
      {
        "name": "Suspicious File Detected",
        "shortName": "Suspicious File Detected",
        "enabled": "false",
        "securityAction": "Block"
      },
      {
        "name": "Privilege Escalation Exploit Detected - A malicious escalation of
privileges was detected",
        "shortName": "Privilege Escalation Exploit Detected",
        "enabled": "true",
        "securityAction": "Block"
      }
    ]
```

```
    }
]
```

resolve-applications (PUT)

This API call enables applications to be resolved/unresolved.

- **Input Parameters:**
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
  - **vendors:** Specifies the list of vendor names. Names must match exactly. **strictMode** is always true.
  - **products:** Specifies the list of product names. Names must match exactly. **strictMode** is always true.
  - **versions:** Specifies the list of versions. Names must match exactly. **strictMode** is always true.
  - **signed:** A true/false parameter indicating if the policy is signed. Possible values are: true, false.
  - **applyNested:** A true/false parameter indicating that updating is inherited. Possible values are: true, false.
  - **comment:** Specifies a user-defined string to attach to the policy.
  - **resolve:** A true/false parameter indicating whether or not to update the application resolve/unresolved state.

Sample Request

https://ENSILOHOST/management-rest/comm-control/resolve-applications

set-policy-rule-state (PUT)

This API call sets the rule in the policy to enable/disable:

- **Input Parameters:**
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
  - **policyName**: Specifies the security policy name.
  - **ruleName:** Specifies the rule name. Possible values are: Vulnerability rule, Reputation rule.
  - **state:** The policy rule state. Possible values are: Enabled, Disabled.

Sample Request:

https://ENSILOHOST/management-rest/comm-control/set-policy-rule-state

System Inventory

The System Inventory module enables you to monitor the health of Fortinet components and to create collector groups.

list-collectors (GET)

This API call outputs a list of the collectors in the system. Use the input parameters to filter the list:

- **Input Parameters –** Can be any combination of these parameters in order to query for data:
  - **devices:** Specifies the list of device names.
  - **devicesIds:** Specifies the list of device IDs.
  - **collectorGroups:** Specifies the list of collector group names and retrieves collectors under the given groups.
  - **ips:** Specifies the list of IP values.
  - **operatingSystems:** Specifies the list of specific operating systems. For example, Windows 7 Pro.
  - **osFamilies:** Specifies the list of operating system families: Windows, Windows Server, OS X.
  - **states:** Specifies the list of collector states: Running, Disconnected, Disabled, Degraded, Pending Reboot, Isolated, Expired, Migrated or Pending Migration.
  - **firstSeen:** Retrieves Collectors that were first seen after this date. Date format: yyyy-MM-dd HH:mm:ss.
  - **lastSeenStart:** Retrieves collectors that were last seen after the value assigned to this date.
    Date Format: yyyy-MM-dd HH:mm:ss.
  - **lastSeenEnd:** Retrieve collectors that were last seen before the value assigned to this date.
    Date Format: yyyy-MM-dd HH:mm:ss.
  - **versions:** Specifies the list of collector versions.
  - **strictMode:** A true/false parameter indicating whether to perform strict matching on the search parameters. The default is False.
  - **pageNumber:** An integer used for paging that indicates the required page number.
  - **itemsPerPage:** An integer used for paging that indicates the number of collectors to retrieve for the current page. The default is 100. The maximum value is 2,000.
  - **sorting:** Specifies a list of strings in JSON format representing the fields by which to sort the results in the following format: "column1":true, "column2":false. True indicates to sort in descending order. Results are sorted by the first field, then by the second field and so on.
  - **showExpired:** A true/false parameter indicating whether to show an expired collector.
  - **loggedUser:** Specifies the user that was logged in when the event occurred.
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the **organization** parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.
  - **hasCrashDumps:** A true/false parameter indicating whether or not to retrieve collectors that have crash dumps.
- **Output Parameters:**
  - **name:** Specifies the name of the collector's device.
  - **id:** Specifies the collector ID.
  - **collectorGroupName:** Specifies the name of the collector group to which the collector belongs.
  - **operatingSystem:** Specifies the operating system of the collector's device.
  - **ipAddress:** Specifies the IP address of the collector's device.
  - **osFamilies:** Specifies the list of operating system families: Windows, Windows Server, OS X.
  - **state:** Specifies the collector’s state: Running, Disconnected, Disabled, Degraded, RebootPending or Isolated.

- **lastSeenTime:** Specifies when the collector was last seen.
  Date Format: yyyy-MM-dd HH:mm:ss.
- **version:** Specifies the collector's version.
- **loggedUsers:** Specifies the logged-in users.
- **macAddresses:** Specifies the list of MAC addresses.
- **accountName:** Specifies the organization name (Deprecated).
- **degradedReason:** Specifies the reason for the degradation.
- **crashDumps:** Collector crash dumps.
- **organization:** Specifies the organization name.
- **stateAdditionalInfo:** Provides additional information about the collector state.
- **systemInformation:** Provides details about the hardware and operating system of the device, such as its CPU, memory, storage and exact OS build and version.

- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

Sample Request

https:// ENSILOHOST/management-rest/inventory/list-collectors?devices=myDevice,myDevice2&collectorGroups=OSX Users,Home Users&ips=1.2.3.4,5.6.7.8&os=windows 7 pro, windows 10 home edition&osFamilies=windows&states=Running,Degraded&lastSeenStart=2016-05-31 00:00:00&lastSeenEnd=2016-06-01 00:00:00&versions=2.0.0,2.0.1

Sample Response


```
[
  {
    "name": "myDevice",
    "collectorGroupName": "Home Users",
    "operatingSystem": "Windows 7 Pro",
    "ipAddress": "10.0.0.7",
    "osFamily": "Windows",
    "state": "Running",
    "lastSeenTime": "2016-06-15 19:10",
    "version": "2.0.0"
  },
  {
    "name": "myDevice2",
    "collectorGroupName": "Home Users",
    "operatingSystem": "Windows 10 Home Edition",
    "ipAddress": "172.16.38.139",
    "osFamily": "Windows",
    "state": "Running",
    "lastSeenTime": "2016-06-15 19:10",
    "version": "2.0.2"
  }
]
```


list-unmanaged-devices(GET)

This API call outputs a list of devices in the environment that have been detected not to have an installed FortiEDR collector. This API is supported from version 5.0 and above.

- **Input Parameters:**
  - **pageNumber:** An integer used for paging that indicates the required page number.
  - **itemsPerPage:** An integer used for paging that indicates the number of collectors to retrieve for the current page. The default is 100. The maximum value is 2,000.
  - **sorting:** Specifies a list of strings in JSON format representing the fields by which to sort the results in the following format: "column1":true, "column2":false. True specifies to sort in descending order. Results are sorted by the first field, then by the second field and so on.
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies, as follows:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.

Sample Request

https://ENSILOHOST/management-rest/inventory/list-unmanaged-devices

Sample Response


```
[
{
  "id" : 2958230,
  "name" : "desktop-tt.ensilo.local",
  "collectorGroupName" : "Unmanaged devices",
  "operatingSystem" : "Windows",
  "ipAddress" : "10.51.102.5",
  "lastSeenTime" : "2020-12-07 03:31:26",
  "macAddresses" : [ "00-15-5D-2E-D4-02" ],
  "accountName" : "ensilofordev",
  "organization" : "ensilofordev",
  "state" : "Unmanaged"
},
{
  "id" : 2958212,
  "name" : "N/A",
  "collectorGroupName" : "Unmanaged devices",
  "operatingSystem" : "Linux (VM)",
  "ipAddress" : "10.51.101.25",
  "lastSeenTime" : "2021-03-30 07:54:58",
  "macAddresses" : [ "00-0C-29-36-B9-68" ],
  "accountName" : "ensilofordev",
  "organization" : "ensilofordev",
  "state" : "Unmanaged"
}
]
```

delete-collectors (DELETE)

This API call deletes a collector(s):

Note – If only collector groups are given as search parameters, all the collectors in the groups are deleted, plus the groups themselves.

- **Input Parameters –** Can be any combination of these parameters in order to query for data:
  - **devices:** Specifies the list of device names.
  - **devicesIds:** Specifies the list of device IDs.
  - **collectorGroups:** Specifies the list of collector group names and retrieves collectors under the given groups.
  - **ips:** Specifies the list of IP values.
  - **operatingSystems:** Specifies the list of specific operating systems. For example, Windows 7 Pro.
  - **osFamilies:** Specifies the list of operating system families: Windows, Windows Server or OS X.
  - **states:** Specifies the list of collector states: Running, Disconnected, Disabled, Degraded, Pending Reboot, Isolated, Expired, Migrated or Pending Migration.
  - **lastSeenStart:** Retrieves collectors that were last seen after the value assigned to this date.

    Date Format: yyyy-MM-dd HH:mm:ss.
  - **lastSeenEnd:** Retrieves collectors that were last seen before the value assigned to this date.

    Date Format: yyyy-MM-dd HH:mm:ss.
  - **versions:** Specifies the list of collector versions.
  - **strictMode:** A true/false parameter indicating whether to perform strict matching on the search parameters. The default is False.
  - **pageNumber:** An integer used for paging that indicates the required page number.
  - **itemsPerPage:** An integer used for paging that indicates the number of collectors to retrieve for the current page. The default is 100. The maximum value is 2,000.
  - **sorting:** Specifies a list of strings in JSON format representing the fields by which to sort the results in the following format: "column1":true, "column2":false. True indicates to sort in descending order. Results are sorted by the first field, then by the second field and so on.
  - **showExpired:** A true/false parameter indicating whether to show an expired collector.
  - **loggedUser:** Specifies the user that was logged in when the event occurred.
  - **deleteAll:** A true/false parameter. True deletes all events. When this value is set to true, no other filtering parameter(s) can be combined in the same request.
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.
  - **hasCrashDumps:** A true/false parameter indicating whether or not to retrieve collectors that have crash dumps.
  - **confirmDeletion:** A true/false parameter indicating whether or not to detach/delete relevant exceptions from collector groups that are about to be deleted.
- **Output Parameters –** None.

  Response code 200 indicates a successful operation.
- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

- Error code 400 is returned if **lastSeenStart** is later than the current date.
- Error code 400 is returned if **lastSeenStart** is later than **lastSeenEnd**.

Note – If only collector groups are given as search parameters, all the collectors in the groups are deleted as well as the groups themselves.

Sample Request

https:// ENSILOHOST/management-rest/inventory/delete-collectors?devices=myDevice,myDevice2&collectorGroups=OSX Users,Home Users&ips=1.2.3.4,5.6.7.8&os=windows 7 pro, windows 10 home edition&osFamilies=windows&states=Running,Degraded&lastSeenStart=2016-05-31 00:00:00&lastSeenEnd=2016-06-01 00:00:00&versions=2.0.0,2.0.1

Request Type: **DELETE**

In the sample request above, all collectors matching the search criteria are deleted (response code 200 OK).

toggle-collectors (PUT)

This API call enables/disables a collector(s). You must specify whether the collector is to be enabled or disabled:

- **Input Parameters –** Can be any combination of these parameters in order to query for data:
  - **enable:** A mandatory true/false parameter indicating whether to enable (true) or disable (false) the collectors.
  - **devices:** Specifies the list of device names.
  - **devicesIds:** Specifies the list of device IDs.
  - **collectorGroups:** Specifies the list of collector group names and retrieves collectors under the given groups.
  - **ips:** Specifies the list of IP values.
  - **operatingSystems:** Specifies the list of specific operating systems. For example, Windows 7 Pro.
  - **osFamilies:** Specifies the list of operating system families: Windows, Windows Server or OS X.
  - **states:** Specifies the list of collector states: Running, Disconnected, Disabled, Degraded, Pending Reboot, Isolated, Expired, Migrated or Pending Migration.
  - **lastSeenStart:** Retrieves collectors that were last seen after the value assigned to this date.

    Date Format: yyyy-MM-dd HH:mm:ss.
  - **lastSeenEnd:** Retrieves collectors that were last seen before the value assigned to this date.

    Date Format: yyyy-MM-dd HH:mm:ss.
  - **versions:** Specifies the list of collector versions.
  - **strictMode:** A true/false parameter indicating whether to perform strict matching on the search parameters. The default is False.
  - **pageNumber:** An integer used for paging that indicates the required page number.
  - **itemsPerPage:** An integer used for paging that indicates the number of collectors to retrieve for the current page. The default is 100. The maximum value is 2,000.
  - **sorting:** Specifies a list of strings in JSON format representing the fields by which to sort the results in the following format: "column1":true, "column2":false. True indicates to sort in descending order. Results are sorted by the first field, then by the second field and so on.
  - **showExpired:** A true/false parameter indicating whether to show an expired collector.
  - **loggedUser:** Specifies the user that was logged in when the event occurred.
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.

- **hasCrashDumps:** A true/false parameter indicating whether or not to retrieve collectors that have crash dumps.

- **Output Parameters –** None.

  Response code 200 indicates a successful operation.

- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.
  - Error code 400 is returned if **lastSeenStart** is later than the current date.
  - Error code 400 is returned if **lastSeenStart** is later than **lastSeenEnd**.

Sample Request

https:// ENSILOHOST/management-rest/inventory/toggle-collectors?enable=true&devices=myDevice,myDevice2&collectorGroups=OSX Users,Home Users&ips=1.2.3.4,5.6.7.8&os=windows 7 pro, windows 10 home edition&osFamilies=windows&states=Running,Degraded&lastSeenStart=2016-05-31 00:00:00&lastSeenEnd=2016-06-01 00:00:00&versions=2.0.0,2.0.1

Request Type: **PUT**

move-collectors (PUT)

- **Input Parameters –** Can be any combination of the parameters in order to query for data:
  - **collectors:** A list of collector device names.

    Note – To move collectors between organizations, the collectors parameter should contain the organization name with a backslash before the name.

    For example, OrgA\collectorA.
    Only a hoster user can move collectors between organizations. In this case, the organization property is mandatory and must have the All organizations value.
  - **targetCollectorGroup:** The target collector group name.

    Note – To move collectors between organizations, the **targetCollectorGroup** parameter should contain the organization name with a backslash before the name.
    For example, OrgA\collectorA.
    Only a hoster user can move collectors between organizations. In this case, the organization property is mandatory and must have the **All organizations** value.
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.
  - **forceAssign:** Indicates whether to force the assignment, even if the organization of the target collector group is under migration.
- **Output Parameters –** None.

  Response code 200 indicates a successful operation.
- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

Sample Request

https://10.0.1.51/management-rest/inventory/move-collectors?collectors=BUILD_PC&targetCollectorGroup=Default Collector Group

Request Type: **PUT**

create-collector-group (POST)

- **Input Parameters:**
  - **name:** Specifies the collector group name. This parameter is mandatory.
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

Sample Request

https:// ENSILOHOST/management-rest/inventory/create-collector-group?name=group1https://10.0.1.51/management-rest/inventory/move-collectors?collectors=BUILD_PC&targetCollectorGroup=Default%20Collector%20Group

list-groups (GET)

This API call outputs the collectors groups (for deprecated, use **list-collector-groups** instead).

- **Errors:**
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

Sample Request

https:// ENSILOHOST/management-rest/inventory/list-groups

Sample Response

```
      [
"group1",
"group2",
"group3"
      ]
```

list-aggregators (GET)

This API call outputs a list of aggregators:

- **Input Parameters:**
  - **names:** Specifies the list of aggregator names.
  - **versions:** Specifies the list of aggregator versions.
  - **ip:** Specifies the aggregator IP.
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that

is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:

- **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
- **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.

- **Output Parameters:**
  - **hostName:** Specifies the aggregator host name.
  - **id:** Specifies the aggregator ID.
  - **ipAddress:** Specifies the aggregator IP.
  - **numOfAgents:** Specifies the number of collectors on the aggregator.
  - **numOfDownAgents:** Specifies the number of collectors that are down on the aggregator.
  - **state:** Specifies the aggregator state.
  - **version:** Specifies the aggregator version.
  - **organization:** Specifies the organization of the aggregator.

Sample Request

https:// ENSILOHOST/management-rest/inventory/list-aggregators

list-cores (GET)

This API call outputs a list of cores:

- **Input Parameters:**
  - **names:** Specifies the list of core names.
  - **versions:** Specifies the list of core versions.
  - **deploymentModes:** Specifies the list of the core's deployment modes.
  - **ip:** Specifies the Core IP.
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.
  - **hasCrashDumps:** A true/false parameter indicating whether or not to retrieve collectors that have crash dumps.
- **Output Parameters:**
  - **deploymentMode:** Specifies the core deployment mode.
  - **ip:** Specifies the core IP.
  - **name:** Specifies the core name.
  - **status:** Specifies the core status.
  - **version:** Specifies the core version.
  - **degradedReason:** Specifies the reason for the degradation.
  - **crashDumps:** Core crash dumps.
  - **organization:** Specifies the organization name.
  - **id:** Specifies the core ID.

Sample Request

https:// ENSILOHOST/management-rest/inventory/list-cores

list-repositories (GET)

This API call outputs the list of repositories (edrs):

- **Output Parameters:**
  - **IpAddress:** Specifies the IP address of the repository.
  - **status:** Specifies the repository status.

Sample Request

https:// RENSILOHOST/management-rest/inventory/list-repositories

collector-logs (GET)

This API call retrieves collector logs:

- **Input Parameters:**
  - **device:** Specifies the name of the collector.
  - **deviceId:** Specifies the ID of the collector.
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
- **Output:** This operation results in a file stream (binary data), which is a *.zip file.

Sample Request

https:// ENSILOHOST/management-rest/inventory/collector-logs

isolate-collectors (PUT)

This API call isolates a collector:

- **Input Parameters:**
  - **deviceIds:** Specifies the list of device IDs.
  - **devices:** Specifies the list of device names.
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.

Sample Request

https:// ENSILOHOST/management-rest/inventory/isolate-collectors

unisolate-collectors (PUT)

This API call un-isolates a collector:

- **Input Parameters:**
  - **deviceIds:** Specifies the list of device IDs.
  - **devices:** Specifies the list of device names.
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.

Sample Request

https:// ENSILOHOST/management-rest/inventory/unisolate-collectors

list-collector-groups (GET)

This API call outputs the collectors groups.

- **Input Parameters:**
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.
- **Output Parameters:** This operation results in a file stream (binary data), which is a *.zip file.
  - **organization:** Specifies the organization name.
  - **name:** Specifies the collector group name.
  - **id:** Specifies the collector group id.
  - **targetVersions:** Specifies the collector group target versions.
- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

aggregator-logs (GET)

This API call retrieves an aggregator's logs.

- **Input Parameters:**
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
  - **Device:** Specifies the name of the device.
  - **deviceId:** Specifies the ID of the device.
- **Output Parameters:** This operation results in a file stream (binary data), which is a *.zip file.

Sample Request

https:// ENSILOHOST/management-rest/inventory/aggregator-logs?device=Device_Name&deviceId=1234

core-logs (GET)

This API call retrieves a core's logs.

- **Input Parameters:**
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
  - **Device:** Specifies the name of the device.
  - **deviceId:** Specifies the ID of the device.
- **Output Parameters:** This operation results in a file stream (binary data), which is a *.zip file.

Sample Request

https:// ENSILOHOST/management-rest/inventory/core-logs?device=Device_Name&deviceId=1234

system-logs (GET)

This API call retrieves system (Central Manager) logs.

- **Input Parameters:** None.
- **Output Parameters:** This operation results in a file stream (binary data), which is a *.zip file.

Sample Request

https:// ENSILOHOST/management-rest/inventory/system-logs

Forensics

The Forensics module facilitates deep analysis into the actual internals of the communicating devices' operating system that led up to an event.

get-event-file (GET)

This API call retrieves a file or memory:

Note – File paths can be specified in a logical or a physical format. For example, **C:\abc (logical)** or **\Device\HarddiskVolume2\Windows\System32\wow64.dll** (physical).

- **Input Parameters –** Can be any combination of these parameters in order to query for data:
  - **rawEventId:** Specifies the ID of the raw event on which to perform the memory retrieval. Long value. This parameter is mandatory.
  - **processId:** Specifies the ID of the process from which to take a memory image.
  - **startRange:** Specifies the memory start range, in Hexadecimal format. This parameter is optional.
  - **endRange:** Specifies the memory end range, in Hexadecimal format. This parameter is optional.
  - **filePaths:** Specifies the list of file paths.
  - **memory:** A true/false parameter indicating whether to retrieve from memory.
  - **disk:** A true/false parameter indicating whether to retrieve from disk.
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
- **Output Parameters –** This operation results in a file stream (binary data), which is a .zip file.
- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

Sample Request

https:// ENSILOHOST/management-rest/forensics/get-event-file?rawEventId=1000000001&processType=32bit&processName=explorer.exe&processId=1234&startRange=0x10000&endRange=0x20000

remediate-device (PUT)

This API kill process deletes a file and/or cleans persistent data.

Note – File and persistence paths must be specified in a logical format. For example, **C:\abc** and not **\Device\HarddiskVolume2\Windows\System32\wow64.dll** (physical).

- **Input Parameters –** Can be any combination of these parameters in order to query for data:
  - **device:** Specifies the name of the device to remediate. You must specify a value for either **device** or **deviceId** (see below).
  - **deviceId:** Specifies the unique identifier (ID) of the device to remediate. You must specify a value for either **deviceId** or **device** (see above).

- **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
- **terminatedProcessId:** Represents the process ID to terminate on the device. Number value.
- **executablesToRemove:** Specifies the list of full paths of executable files (*.exe) to delete on the given device.
- **processName:** Specifies the process name.
- **persistenceDataAction:** Specifies the action for the persistent data. Possible values are **DeleteKey**, **DeleteValue** or **Update**.
- **persistenceDataPath:** Specifies the persistent data path.
- **persistenceDataValueName:** Specifies the persistent data value name.
- **persistenceDataNewContent:** Specifies the persistent data new content. The content format provided depends on the type used in **persistenceDataValueNewType** (see below). The format should be provided as follows:
  - **String** for the following types: REG_SZ(1), REG_EXPAND_SZ(2), REG_DWORD(4) and REG_QWORD(11).
  - **Base64** for the following types: REG_BINARY(3), REG_DWORD_BIG_ENDIAN(5), REG_LINK(6), REG_MULTI_SZ(7), REG_RESOURCE_LIST(8), REG_FULL_RESOURCE_DESCRIPTOR(9) and REG_RESOURCE_REQUIREMENTS_LIST(10).
- persistenceDataValueNewType: Specifies the new persistent data value type. Possible values are REG_SZ, REG_EXPAND_SZ, REG_BINARY, REG_DWORD, REG_DWORD_BIG_ENDIAN, REG_LINK, REG_MULTI_SZ, REG_RESOURCE_LIST, REG_FULL_RESOURCE_DESCRIPTOR, REG_RESOURCE_REQUIREMENTS_LIST or REG_QWORD.
- **threadId:** Specifies the thread ID.

- **Output Parameters –** None.

  A text message indicating that the operation completed successfully is returned.

  In case of error, a text message stating the error is returned. This message specifies the file that cannot be deleted.

Sample Request

https:// ENSILOHOST/management-rest/forensics/remediate-device?device=myDevice&terminatedProcessId=1234&executablesToRemove=c:\filecryptor.exe

get-file (GET)

This API call retrieves a file or memory:

- **Input Parameters:**
  - **filePaths:** Specifies the list of file paths. This parameter is mandatory.
  - **type:** Specifies the type of the device input parameter, which can be either **ID** or **NAME**.
  - **device:** Specifies the name or ID of the device to remediate.
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
- **Output Parameters:** This operation results in a file stream (binary data), which is a .zip file.

Sample Request

https:// ENSILOHOST/management-rest/forensics/get-file

Audit

The Audit module enables the retrieval of the FortiEDR audit log.

get-audit (GET)

This API call enables you to retrieve the FortiEDR audit log of a specified time period.

- **Input Parameters:**
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.
  - **fromTime**: Retrieves audit messages that were written after the specified date using the yyyy-MM-dd date format. The default is the current date.
  - **toTime**: Retrieves audit messages that were written before the specified date using the yyyy-MM-dd date format. The default is the current date
- **Output Parameters:** For each audit log entry that matches the query, the following parameters are exported:
  - **dateAndTime**: Specifies the date and time in the format yyyy-mm-dd hh:mm:ss.
  - **description:** Specifies the audited action and/or a description.
  - **subsystem:** Specifies the change type, such as System, Configuration, Administration, Forensics, Events, Inventory or Communication Control.
  - **username**: Specifies the name of the user that performed the audited action.

Sample Request

https://ENSILOHOST/management-rest/audit/get-audit?organization=DEMO

Administrator

The Administrator module enables administrators to perform administrative operations, such as handling licenses and users.

set-system-mode (PUT)

This API call enables you to switch the system to Simulation mode:

- **Input Parameters:**
  - **mode:** Specifies the mode: Simulation or Prevention. This parameter is mandatory.
  - **forceAll:** Supported starting version 3.0.0. Indicates whether to force set all the policies in Prevention mode. This parameter is irrelevant when mode = Simulation. This parameter is optional.
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.
- **Output Parameters –** None.

  Response code 200 OK indicates a successful operation.
- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

Sample Request

https://ENSILOHOST/management-rest/admin/set-system-mode?mode=simulation

list-system-summary (GET)

This API call gets a summary of the environment:

- **Input Parameters:**
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.
  - **addLicenseBlob:** Indicates whether to add the license blob to the response. By default, **addLicenseBlob** is false.
- **Output Parameters:**
  - **workstationCollectorsLicenseCapacity:** Specifies the workstation collector's license capacity.
  - **serverCollectorsLicenseCapacity:** Specifies the server collector's license capacity.
  - **registeredCollectors:** Specifies the registered collectors.
  - **workstationsCollectorsInUse:** Specifies the workstation collectors in use.

- **serverCollectorsInUse:** Specifies the server collectors in use.
- **collectorsState:** Specifies the collector's state: Running, Disconnected, Disabled, Degraded or RebootPending, and provides a count for each of them.
- **licenseExpirationDate:** Specifies the license expiration date.
- **ContentVersion:** Specifies the content version.
- **managementVersion:** Specifies the management version.
- **collectorVersions:** Specifies the list of collector versions.
- **coreVersions:** Specifies the list of core versions.
- **aggregatorVersions:** Specifies the list of aggregators' versions.
- **cores:** Specifies the list of cores. Each core holds the following parameters (supported in V2.7.3 and above):
  - **name:** Specifies the core device name.
  - **address:** Specifies the core IP address.
  - **version:** Specifies the core version.
  - **status:** Indicates the status of the core: Enabled/Degraded.
- **aggregators:** Specifies the list of aggregators. Each aggregator holds the following parameters (supported in V2.7.3 and above):
  - **name:** Specifies the aggregator device name.
  - **address:** Specifies the aggregator IP address.
  - **version:** Specifies the aggregator version.
  - **status:** Indicates the status of the aggregator: Enabled/Degraded.
- **systemState:** Indicates the system state: Protection/Simulation (supported in V2.7.3 and above).
- **customerName:** Specifies the customer name.
- **licenseFeatuers:** Specifies the license features assigned to you, which can include the following:
  - Threat Hunting
  - Forensics
  - Communication Control
  - Protect Anywhere
  - eXtended Detection
  - IoT
  - Vulnerability
- **licenseType:** Specifies the license type. Possible values are – Discover, Protect and Response, Discover, Protect and Response [On-Premise], Discover and Protect or Protect and Response.
- **repositoryAddOns:** Specifies the quantity of Threat Hunting repository add-ons that are included.
- **installationId:** Specifies the installation ID.
- **collectorVersionsV2:** Specifies the collector versions with counts per version.
- **collectorsDegradedState:** Specifies the collector's degraded state: FailedConfigurationUpdate, GatewayUnreachable, PAEDisabled, ContentUpdateError, unsupportedOSVersion, DriverLoadFailure, ApproveKernelExtensions, NoConfiguration, NoDiskSpace, MissingMiniFilterSupport, OTIFailed and provides a count for each of them.
- **collectorsWithDumps:** Specifies the collectors that have crash dumps (NsloCollectorService, NsloCollector, WindowsKernelMini, WindowsKernelFull, LinuxKernelPanic, MacOSKernelPanic) and provides a count for each of them.
- **time:** Specifies the current server time.
- **timeZone:** Specifies the current server timezone.
- **collectorsRunningState:** Specifies the collectors' running state (autonomously, core) and provides a count for each of them.
- **collectorsDisconnectedState:** Specifies the collectors' disconnected state (disconnected, expired, migrated, pending migrated) and provides a count for each of them.
- **managementHostname:** Specifies the management host name.
- **repositories:** Specifies the list of repositories. Each repository holds the following parameters (supported in V4.0 and above):

        - **address:** Specifies the repository IP address.
        - **status:** Indicates the status of the repository (Running/Disconnected).
    - **environmentUniqueId:** Specifies the management ID as defined in ECS.
    - **licenseBlob:** Specifies the license blob.
    - **ecsStatus:** Specifies the ECS status. Possible values are Disabled, Enabled, Degraded and Down.
    - **ecsStatusMessage:** Specifies the ECS status details.
    - **ecsRegistrationURL:** Specifies the ECS registration URL.
    - **iotDevicesInUse:** Specifies the IoT devices in use.
    - **iotDevicesLicenseCapacity:** Specifies the IoT device's license capacity.
    - **managementExternalIP:** Specifies the management external IP.
    - **managementInternalIP:** Specifies the management internal IP.
- **Errors:**
    - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

Sample Request

https://ENSILOHOST/management-rest/admin/list-system-summary

Sample Response


```
{
  "workstationCollectorsLicenseCapacity": 10000,
  "serverCollectorsLicenseCapacity": 10000,
  "registeredCollectors": 6006,
  "workstationsCollectorsInUse": 6003,
  "serverCollectorsInUse": 3,
  "collectorsState": {
    "Degraded": 1,
    "Disabled": 0,
    "Disconnected": 6001,
    "RebootPending": 0,
    "Running": 4,
    "Uninstalling": 0
  },
  "collectorsDegradedState": {
    "ApproveKernelExtensions": 0,
    "ContentUpdateError": 0,
    "DriverLoadFailure": 1,
    "FailedConfigurationUpdate": 0,
    "GatewayUnreachable": 0,
    "NoConfiguration": 0,
    "NoDiskSpace": 0,
    "PAEDisabled": 0,
    "unsupportedOSVersion": 0
  },
  "collectorsRunningState": {
    "autonomously": 0,
    "core": 4
  },
  "collectorsDisconnectedState": {
    "disconnected": 6001,
    "expired": 0,
```

```
    "migrated": 0,
    "pendingMigration": 0
  },
  "collectorsWithDumps": {
    "LinuxKernelPanic": 0,
    "MacOSKernelPanic": 0,
    "NsloCollector": 0,
    "NsloCollectorService": 0,
    "WindowsKernelFull": 0,
    "WindowsKernelMini": 0
  },
  "licenseExpirationDate": "11-Sep-2020",
  "managementVersion": "4.0.0.62",
  "managementHostname": "",
  "collectorVersions": [
    "3.1.1.40",
    "3.1.1.487",
    "4.0.0.45"
  ],
  "collectorVersionsV2": [
    {
      "count": 2,
      "version": "3.1.1.40"
    }
  ],
  "cores": [
    {
      "name": "ensilo-core-friendly-awaited-hound",
      "address": "10.51.121.182:555",
      "version": "4.0.0.50",
      "status": "Enabled"
    },
    {
      "name": "ensilo-core-neatly-close-crawfish",
      "address": "10.51.121.172:555",
      "version": "4.0.0.50",
      "status": "Enabled"
    }
  ],
  "aggregators": [
    {
      "name": "ensilo",
      "address": "127.0.0.1:8081",
      "version": "4.0.0.62",
      "status": "Enabled"
    }
  ],
  "repositories": [
    {
      "address": "10.51.121.164:443",
```

```
      "status": "Running"
    }
  ],
  "systemState": "Protection",
  "customerName": "Default",
  "licenseFeatures": [
    "Protect Anywhere",
    "Communication Control",
    "Forensics",
    "Thread Hunting"
  ],
  "licenseType": "Discover, Protect and Response",

  "installationId": 1948046639,
  "time": "2019-09-24 14:56:19",
  "timeZone": "UTC +03:00",
  "environmentUniqueId": "JonathanGolfCVE_1948046639",
  "ecsStatus": "Enabled",
  "repositoryAddOns": 0,
  "contentVersion": "3977"
}
```


upload-content (POST)

This API call uploads content to the system:

- **Input Parameter:**
  - **file:** Specifies the content file. This parameter is mandatory.

export-organization (GET)

This API call exports organizational data as a zip file.

- **Input Parameters:**
  - **organization:** Specifies the organization to export. This parameter is mandatory.
  - **destinationName:** Specifies the organization's destination name.
- **Output Parameters –** This operation results in a file stream (binary data), which is a *.zip file.
- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

Sample Request

https://ENSILOHOST/management-rest/admin/export-organization?organization=orgA&destinationName=orgB

import-organization (POST)

This API call imports an organization.

- **Input Parameters:**
  - **file:** Specifies the content file. This parameter is mandatory.
- **Output Parameters:**
  - **organization:** Specifies the organization name.
  - **organizationId:** Specifies the organization ID.

- **verificationCode:** Imports the verification code.

- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

Sample Request

https://ENSILOHOST/management-rest/admin/import-organization

transfer-collectors (POST)

This API call transfers collectors from aggregator to aggregator during an organization migration process.

- **Body Parameters:**
  - **verificationCode:** Specifies the verification code to validate that the import step finished successfully. This parameter is mandatory.
  - **sourceOrganization:** Specifies the organization from which collectors will be transferred. This parameter is mandatory.
  - **targetOrganization:** Specifies the organization to which collectors will be transferred. This parameter is mandatory.
  - **aggregatorsMap:** Specifies the aggregator transfer mapping, as follows:
    - **sourceAggregatorId:** Specifies the source aggregator ID. This parameter is mandatory.
    - **targetAggregatorDestination**: Specifies the target aggregator destination IP or DNS. This parameter is mandatory.
    - **targetAggregatorPort:** Specifies the target aggregator destination port. This parameter is mandatory.
- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

Sample Request

https://ENSILOHOST/management-rest/admin/transfer-collectors

Request Body:

```
{
   sourceOrganization: "orgA",
   targetOrganization: "orgB",
   verificationCode: 12345,
   aggregatorsMap {
         sourceAggregatorId: 111,
         targetAggregatorDestination: "1.1.1.1",
         targetAggregatorPort: 8081
   }
}
```

transfer-collectors-stop (POST)

This API call stops the transfer of collectors during a migration process.

- **Input Parameters:**
  - **organization:** Specifies the organization whose migration process should be stopped.
- **Errors:**

- Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
- Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

Sample Request

https://ENSILOHOST/management-rest/admin/transfer-collectors-stop?organization=orgA

list-collector-installers (GET)

This API call outputs the available collector installers:

- **Input Parameters:**
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.
- **Output Parameters –** Response code 200 OK indicates a successful operation.
  - **availableCollectorInstallers:** Specifies the available collector installers.

Sample Request

https://ENSILOHOST/management-rest/admin/list-collector-installers

Sample Response


```
{
  "availableCollectorInstallers": [
    {
      "osFamily": "OSX",
      "version": "3.0.1.119"
    }
  ]
}
```

update-collector-installer (POST)

This API call updates the collectors' target version for collector groups.

- **Input Parameters:**
  - **collectorGroups:** Specifies the list of all the collector groups to be updated.
  - **collectorGroupIds:** Specifies the list of IDs of all the collector groups to be updated.
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.
- **Body Input Parameters:**
  - **updateVersions:** Provides a list of installer versions to be applied in the collector groups.

Sample Request

https://ENSILOHOST/management-rest/admin/update-collector-installer?collectorGroups=Default Collector Group

Sample Body

```
{
"updateVersions": [
{ "osFamily": "Windows", "version": "4.0.0.106" },
{ "osFamily": "OSX", "version": "3.1.0.63" },
{ "osFamily": "Linux", "version": "3.1.1.40" }
]
}
```

upload-license (PUT)

This API call uploads a license to the system:

- **Input Parameters:**
  - **license:** Specifies the license.
- **Body Input Parameters:**
  - **licenseBlob:** Specifies the license blob.

Sample Request

https://ENSILOHOST/ management-rest/admin/upload-license

Sample Body

```
{
    "licenseBlob": "<string>"
}
```

System Events

list-system-events (GET)

Note – This command is supported in the Central Manager V2.6 and above.

- **Input Parameters –** Can be any combination of these parameters in order to query for data:
  - **componentNames:** Specifies one or more names. The name is the customer name for license-related system events and the device name for all others events.
  - **componentTypes:** Specifies one or more component type, which can be any of the following:
    - License
    - Core
    - Aggregator
    - Collector
    - ECS
    - Manager
    - EDR
  - **fromDate:** Searches for system events that occurred after this date.

    Date Format: yyyy-MM-dd HH:mm:ss.
  - **toDate:** Searches for system events that occurred before this date.

    Date Format: yyyy-MM-dd HH:mm:ss.
  - **strictMode:** A true/false parameter indicating whether or not to perform strict matching on the search parameters. The default is false.
  - **pageNumber:** An integer used for paging. This value indicates the required page number. The Page Index starts at 0. The default is 0.
  - **itemsPerPage:** An integer used for paging. This value indicates how many system events to retrieve for the current page. The default is 100 and the maximum is 2,000.
  - **sort:** Specifies a list of strings in JSON format representing the fields by which to sort the results in the following format: {'column1': true, 'column2': false}.

    The true/false indicates value whether the sort is in descending or ascending order. True indicates to sort in descending order. The results are sorted by the first field, then by the second field and so on.

    Available columns are componentType, componentName, description and date.
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.
- **Output Parameters –** Exports the following parameters for each event that matches the query:
  - **componentName:** Specifies the name of the main process of the event.
  - **componentType:** Specifies the target component type that generated the system event.
  - **description:** Provides a description of the system event.
  - **date:** Specifies the full date and time when the system event occurred.
  - **organization:** Specifies the organization of the system event.
- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.

- Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.
- Error code 400 is returned if the **fromDate** is later than the **toDate**.

Sample Request

https://localhost/management-rest/system-events/list-system-events?componentNames=ensilo,USER-PC&componentTypes=Aggregator,Core&fromDate=2017-05-27 00:00:00&toDate=2017-05-28 00:00:00

Sample Response


```
[ {
    "componentName": "USER-PC",
    "componentType": "Core",
    "description": "Core \"USER-PC\" state was changed to \"Running\" ",
    "date": "28-May-2017, 14:36:49"
  },
  {
    "componentName": "ensilo",
    "componentType": "Aggregator",
    "description": "Aggregator \"ensilo\" state was changed to \"Running\"",
    "date": "28-May-2017, 14:36:38"
  },
  {
    "componentName": "ensilo",
    "componentType": "Aggregator",
    "description": "Aggregator \"ensilo\" state was changed to \"Disconnected\"",
    "date": "28-May-2017, 14:36:37"
  },
  {
    "componentName": "USER-PC",
    "componentType": "Core",
    "description": "Core \"USER-PC\" state was changed to \"Disconnected\" ",
    "date": "28-May-2017, 14:36:37"
  }]
```

Policies

clone (POST)

This API call clones a policy:

- **Input Parameters:**
  - **sourcePolicyName:** Specifies the security policy name. This parameter is mandatory.
  - **newPolicyName:** Specifies the security policy name. This parameter is mandatory.
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

Sample Request

https://ENSILOHOST/management-rest/policies/clone?sourcePolicyName=Execution Prevention&newPolicyName=myPolicy

set-mode (PUT)

This API call sets a specific policy to Simulation/Prevention mode:

- **Input Parameters:**
  - **policyName:** Specifies the security policy name. This parameter is mandatory.
  - **mode:** Specifies the mode (Simulation/Prevention). This parameter is mandatory.
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

Sample Request

https://ENSILOHOST/management-rest/policies/set-mode?policyName=Execution Prevention&mode=Prevention

set-policy-rule-action (PUT)

This API call sets a specific rule in a policy to Block or Log:

- **Input Parameters:**
  - **policyName:** Specifies the security policy name. This parameter is mandatory.
  - **ruleName:** Specifies the rule name. This parameter is mandatory.
  - **action:** Specifies the policy action: Log, Block, SimulationBlock, Ignore or Accept. This parameter is mandatory.
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

Sample Request

https://ENSILOHOST/management-rest/policies/set-policy-rule-action?policyName=Execution Prevention&ruleName=Malicious File Detected&action=SimulationBlock

assign-collector-group (PUT)

This API call assigns a collector group to an existing policy:

- **Input Parameters:**
  - **policyName:** Specifies the security policy name. This parameter is mandatory.
  - **collectorsGroupName:** Specifies the list of collector group names.
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
  - **forceAssign:** Indicates whether to force the assignment even, if the group is assigned to similar policies.
- **Output Parameters:**
  - **ignoredCollectorGroupsNames:** Specifies the list of collector groups already assigned to the policy.
- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

Sample Request

https://ENSILOHOST/management-rest/policies/assign-collector-group?policyName=Execution Prevention&collectorsGroupName=myGroup

Sample Response

```
{
   "ignoredCollectorGroupNames": [
   "aa"
   ]
}
```

set-policy-rule-state (PUT)

This API call sets a rule in a policy to enable/disable:

- **Input Parameters:**
  - **policyName:** Specifies the security policy name. This parameter is mandatory.
  - **ruleName:** Specifies the rule name. This parameter is mandatory.
  - **state:** Specifies the policy state: Enabled or Disabled. This parameter is mandatory.
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

Sample Request

https://ENSILOHOST/management-rest/policies/set-policy-rule-state?policyName=Execution Prevention&ruleName=Malicious File Detected&state=Disabled

list-policies (GET)

This API call outputs a list of policies (supported in V2.7.3 and above):

- **Input Parameters:**
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.
- **Output Parameters:**
  - **name:** Specifies the policy name.
  - **operationMode:** Specifies the policy mode (Simulation/Prevention).
  - **agentGroups:** Specifies the list of agent group names to which the policy applies.
  - **organization:** Specifies the organization of the policy.
  - **rules:** Specifies the list of rules included in the policy:
    - **name:** Specifies the rule name.
    - **enabled:** Indicates whether the rule is enabled: true or false.
    - **securityAction:** Specifies the rule security action to apply: Log, Block, SimulationBlock, Ignore or Accept.
    - **shortName:** Specifies the rule short name.
- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

Sample Request

https://ENSILOHOST/management-rest/policies/list-policies

Sample Response


```
[
{
            "name": "Ransomware Prevention",
            "operationMode": "Prevention",
            "agentGroups":
               [
                 "group1",
                 "group2"
               ],
            "rules":
               [
                  {
                     "securityAction": "Block",
                     "name": "Process Hollowing - Process Code Was Replaced",
                     "enabled": "true"
                  }
               ]
}
]
```

IP Sets

list-ip-sets (GET)

This API call outputs a list of IP Sets:

- **Input Parameters:**
  - **ip:** Specifies the IPs contained in the group.
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the **organization** parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.
- **Output Parameters:**
  - **name:** Specifies the IP Set name.
  - **description:** Specifies the IP Set description.
  - **include:** Specifies the list of IPs to include.
  - **exclude:** Specifies the list of IPs to exclude.
  - **organization:** Specifies the organization that created the IP Set (only for an Administrator role).

Sample Request

https://ENSILOHOST/management-rest/ip-sets/list-ip-sets?ip=1.1.1.1&organization=admin

Sample Response


```
[
{
"name": "Internal Destinations",
"description": "APIdescription",
"include": [
"10.0.0.0/8",
"169.254.0.0/16",
"172.16.0.0/12",
"192.168.0.0/16",
"FC00::/7",
"fe80::/10",
"7.7.7.7"
],
"exclude": [
"2.2.2.2",
"9.9.9.9",
"1.1.1.1-5.5.5.5"
]
},
{
"name": "aaa",
"description": "API description",
"include": [
"1.1.1.1",
"7.7.7.7"
],
```

```
"exclude": [
"2.2.2.2",
"3.3.3.3",
"4.4.4.4",
"9.9.9.9"
]
}
]
```

create-ip-set (POST)

This API call creates an IP Set:

- **Body Parameters:**
  - **name:** Specifies IP set name.
  - **description:** Specifies the IP set description.
  - **include:** Specifies the list of IPs to include.
  - **exclude:** Specifies the list of IPs to exclude.
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.
    - **each:** Indicates that the operation applies independently to each organization. For example, let's assume that the same user exists in multiple organizations. When each is specified in the organization parameter, then each organization can update this user separately.

Sample Request

https://ENSILOHOST/management-rest/ip-sets/create-ip-sethttps://ensilohost/management-rest/ip-sets/list-ip-sets?ip=1.1.1.1&organization=admin

Sample Response

```
body
{
"name": "aaa",
"description": "APIdescription",
"include": ["2.2.2.2", "1.2.3.4"],
"exclude":["5.5.5.5", "1.1.1.1-2.2.2.2"],
"organization": "admin"
}
```

update-ip-set (PUT)

This API call updates an IP Set:

- **Input Parameter:**
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that

is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:

- **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
- **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.
- **each:** Indicates that the operation applies independently to each organization. For example, let's assume that the same user exists in multiple organizations. When each is specified in the organization parameter, then each organization can update this user separately.

- **Body Input Parameters:**
  - **name:** Specifies the IP Set name.
  - **description:** Specifies the IP Set description.
  - **include:** Specifies the list of IPs to include.
  - **exclude:** Specifies the list of IPs to exclude.
- **Output Parameters:**
  - **name:** Specifies the IP Set name.
  - **description:** Specifies the IP Set description.
  - **include:** Specifies the list of IPs to include.
  - **exclude:** Specifies the list of IPs to exclude.
  - **organization:** Specifies the organization that created the IP Set (relevant only for an Administrator role).

Sample Request

https://ENSILOHOST/management-rest/ip-sets/update-ip-set?organization:All organizations

Sample Response

```
body
{
"name": "aaa",
"description": "APIdescription",
"include": ["7.7.7.7", "1.1.1.1"],
"exclude":["9.9.9.9", "2.2.2.2", "3.3.3.3"]
}
```

delete-ip-set (DELETE)

This API call deletes an IP Set:

- **Input Parameters:**
  - **ipSets:** Specifies the list of IP Set names.
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.

Sample Request

https://ENSILOHOST/management-rest/ip-sets/delete-ip-set?ipSets=a,a1,a2&organization=admin

Organizations

list-organizations (GET)

This API call outputs a list of organizations:

- **Output Parameters:**
  - **expirationDate:** Specifies the expiration date.
  - **isAdminAccount:** Indicates whether or not the account is an administrator account.
  - **name:** Specifies the account name.
  - **serversAllocated:** Specifics the servers allocated.
  - **serversInUse:** Specifics the server account in use.
  - **workstationsAllocated:** Specifies the workstations allocated.
  - **workstationsInUse:** Specifies the workstation account in use.
  - **verificationCode:** Specifies the organization migration verification code.
  - **iotAllocated:** Specifies the IoT devices allocated.
  - **iotInUse:** Specifies the IoT device account in use.
  - **forensicsAndEDR:** A true/false parameter indicating whether the organization has the Forensics and Threat Hunting license add-on.
  - **vulnerabilityAndIoT:** A true/false parameter indicating whether the organization has the Vulnerability and IoT license add-on.
  - **eXtendedDetection:** A true/false parameter indicating whether the organization has the eXtended Detection license add-on.
  - **repositoryAddOns:** Specifies how many Threat Hunting repository add-ons have been allocated.
  - **organizationId:** Specifics the organization ID.

Sample Request

https://ENSILOHOST/management-rest/organizations/list-organizations

Sample Response


```
{
        "name": "TestTenant",
        "organizationId": 4803078,
        "workstationsAllocated": 0,
        "serversAllocated": 0,
        "iotAllocated": 0,
        "workstationsInUse": 0,
        "serversInUse": 0,
        "iotInUse": 0,
        "expirationDate": "2021-08-30",
        "vulnerabilityAndIoT": true,
        "forensicsAndEDR": true,
        "verificationCode": null,
        "eXtendedDetection": false,
        "repositoryAddOns": 0,
        "isAdminAccount": true
 }
```


create-organization (POST)

This API call creates an organization in the system (only available for API user with Admin role):

- **Body Input Parameters:**

- **expirationDate:** Specifies the license expiration date. Specify the date using the following date format: yyyy-MM-dd.
- **name:** Specifies the organization name.
- **password:** Specifies the device registration password name.
- **passwordConfirmation:** Specifies the confirm device registration password name.
- **serversAllocated:** Specifies the server collector's license capacity.
- **workstationsAllocated:** Specifies the workstation collector's license capacity.
- **iotAllocated:** Specifies the IoT device's license capacity.
- **forensicsAndEDR:** A true/false parameter indicating whether the organization has the Forensics and Threat Hunting license add-on.
- **vulnerabilityAndIoT:** A true/false parameter indicating whether the organization has the Vulnerability And IoT license add-on.

Sample Request

https://ENSILOHOST/management-rest/organizations/create-organization

Sample Body

```
{
    "expirationDate": "01/09/2021”
    "name": "newOrg",
    "password": "1234",
    "passwordConfirmation": "1234",
    "serversAllocated": "10",
    "workstationsAllocated": "15”
}
```

delete-organization (DELETE)

This API call deletes an organization in the system (only available for API user with Admin role)

- **Input Parameters:**
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.

Sample Request

https://ENSILOHOST/management-rest/organizations/delete-organization?organization=orgName

update-organization (PUT)

This API call updates an organization in the system (only available for API user with Admin role)

- **Input Parameters:**
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
- **Body Input Parameters:**
  - **expirationDate:** Specifies the license expiration date. Specify the date using the following date format: yyyy-MM-dd.
  - **name:** Specifies the organization name.
  - **serversAllocated:** Specifies the server collector's license capacity.
  - **workstationsAllocated:** Specifies the workstation collector's license capacity.
  - **iotAllocated:** Specifies the IoT device's license capacity.
  - **forensicsAndEDR:** A true/false parameter indicating whether the organization has the Forensics and Threat Hunting license add-on.

- **vulnerabilityAndIoT:** A true/false parameter indicating whether the organization has the Vulnerability And IoT license add-on.

Sample Request

https://ENSILOHOST/management-rest/organizations/update-organization?organization=orgName

Sample Body

```
{
"expirationDate": "string",
"forensicsAndEDR": false,
"iotAllocated": 0,
"name": "string",
"serversAllocated": 0,
"vulnerabilityAndIoT": false,
"workstationsAllocated": 0
}
```

Users

create-user (POST)

This API call creates a user:

- **Input Parameter:**
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **each:** Indicates that the operation applies independently to each organization. For example, let's assume that the same user exists in multiple organizations. When each is specified in the organization parameter, then each organization can update this user separately.
- **Body Input Parameters:**
  - **username:** Specifies the login username of the user. This parameter is mandatory.
  - **firstName:** Specifies the first name of the user. This parameter is mandatory.
  - **lastName:** Specifies the last name of the user. This parameter is mandatory.
  - **email:** Specifies the email address of the user. This parameter is mandatory.
  - **password:** Specifies the login password of the user. This parameter is mandatory.
  - **confirmPassword:** Specifies the confirm password of the user. This parameter is mandatory.
  - **title:** Specifies the title of the user.
  - **roles:** Specifies the roles of the user. Possible values are **Admin**, **Local Admin**, **User** or **Rest API**. This parameter is mandatory.

Sample Request

https://ENSILOHOST/management-rest/users/create-user

Sample Response

```
body
{
"email": "bob@ensilo.com",
,firstName": "bob
"lastName": "dan,
"roles": [
"Admin"
],
"title": "admin user",
"username": "bob"
"confirmPassword": "12345678",
"password": "12345678",
}
```

delete-user (DELETE)

This API call deletes a user(s):

- **Input Parameters:**
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
  - **username:** Specifies the name of the user. This parameter is mandatory.

Sample Request

https://ENSILOHOST/management-rest/users/delete-user?username=bob

list-users (GET)

This API call outputs a list of users:

- **Input Parameter:**
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.
- **Output Parameters:**
  - **username:** Specifies the login username of the user.
  - **firstName:** Specifies the first name of user.
  - **lastName:** Specifies the last name of user.
  - **email:** Specifies the email address of the user.
  - **title:** Specifies the title of the user.
  - **roles:** Specifies the roles of the user. Possible values are **Admin**, **Local Admin**, **User** and **Rest API**.
  - **id:** Specifies the ID of the user.
  - **organization:** Specifies the organization of the user.

Sample Request

https://ENSILOHOST/management-rest/users/list-users

Sample Response


```
[
{
"organization": "Default",
"id": 10,
"username": "admin",
"roles": [
"User",
"Rest API",
"Admin",
"Local Admin"
],
"firstName": "aaa",
"lastName": "aaa",
"title": null,
"email": "aaa@aa.com"
}
]
```


reset-password (PUT)

This API call resets a user's password:

- **Input Parameters:**
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
  - **username:** Specifies the name of the user. This parameter is mandatory.
- **Body Input Parameters:**
  - **password:** Specifies the login password of the user. This parameter is mandatory.
  - **confirmPassword:** Specifies the confirmation password of the user. This parameter is mandatory.

Sample Request

https://ENSILOHOST/management-rest/users/reset-password?username=bob

Sample Response


```
body
{
"confirmPassword": "12345678",
"password": "12345678"
}
```


update-user (PUT)

This API call updates a user:

- **Input Parameters:**
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.

        - **each:** Indicates that the operation applies independently to each organization. For example, let's assume that the same user exists in multiple organizations. When each is specified in the organization parameter, then each organization can update this user separately.
    - **username:** Specifies the name of the user. This parameter is mandatory.
- **Body Input Parameters:**
    - **username:** Specifies the login username of the user. This parameter is mandatory.
    - **firstName:** Specifies the first name of the user. This parameter is mandatory.
    - **lastName:** Specifies the last name of the user. This parameter is mandatory.
    - **email:** Specifies the email address of the user. This parameter is mandatory.
    - **title:** Specifies the title of the user.
    - **roles:** Specifies the roles of the user. Possible values are **Admin**, **Local Admin**, **User** and **Rest API**. This parameter is mandatory.

Sample Request

https://ENSILOHOST/management-rest/users/update-user?username=bob

Sample Response

```
body
{
"email": "bob@ensilo.com",
,firstName": "bob
"lastName": "dan,
"roles": [
"Admin"
],
"title": "admin user",
"username": "bob"
}
```

update-saml-settings (POST)

This API call creates or updates SAML authentication settings. This API is supported from version 5.0 and above.

- **Input Parameters:**
    - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
        - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **enabled:** Specifies whether SAML authentication is enabled.
    - **description:** A free text description of SAML authentication using the configured SAML identity provider.
    - **ssoUrl:** Specifies the SSO URL postfix. This URL will be used for logging into FortiEDR with SAML users.
    - **metadataUrl:** Specifies the IDP metadata URL path. Use either URL or file to get SP metadata.
    - **idpMetadataFile:** Specifies the IDP metadata file. Use either URL or file to get SP metadata.
    - **groupAttribute:** Specifies the name of the attribute to be read by FortiEDR in order to determine the permissions and role to be assigned to that user in FortiEDR.
    - **apiGroupName:** Specifies the attribute value for a user with an API role.
    - **hostGroupName:** Specifies the attribute value for a user with an Admin (hoster) role.
    - **localAdminGroupName:** Specifies the attribute value for a user with a Local Admin role.
    - **usersGroupName:** Specifies the attribute value for a user with a User role.

Sample Request

https://ENSILOHOST/management-rest/users/update-saml-settings

delete-saml-settings (POST)

This API call deletes the SAML authentication settings of a specific organization.

- **Input Parameters:**
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.

Sample Request

https://ENSILOHOST/management-rest/users/delete-saml-settings?organization=DEMO

get-sp-metadata (GET)

This API call retrieves the FortiEDR SP SAML metadata of a specific organization. The response specifies the URL address from which the metadata can be downloaded.

- **Input Parameters:**
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.

Sample Request

https://ENSILOHOST/management-rest/users/get-sp-metadata?organization=DEMO

Sample Response

https:// ENSILOHOST/saml/metadata/alias/1111111

Playbooks

clone (POST)

This API call clones a policy:

- **Input Parameters:**
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
  - **sourcePolicyName:** Specifies the source playbook policy name.
  - **newPolicyName:** Specifies the target playbook policy name.
- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

For this API call, the **organization** parameter only supports the name of a specific organization. The value that you specify for the organization must match exactly.

Sample Request

https://ENSILOHOST/management-rest/playbooks-policies/clone?sourcePolicyName=playbooks&newPolicyName=myPolicy

set-mode (PUT)

This API call sets the policy to Prevention/Simulation mode:

- **Input Parameters:**
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
  - **policyName:** Specifies the security policy name.
  - **mode:** Specifies the mode (Prevention/Simulation). This parameter is mandatory.
- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

For this API call, the **organization** parameter only supports the name of a specific organization. The value that you specify for the organization must match exactly.

Sample Request

https://ENSILOHOST/management-rest/playbooks-policies/set-mode?policyName=playbook&mode=Prevention

assign-collector-group (PUT)

This API call assigns a collector group to a policy:

- **Input Parameters:**
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
  - **policyName:** Specifies the security policy name. This parameter is mandatory.
  - **collectorGroupNames:** Specifies the list of collector group names.
  - **forceAssign:** Indicates whether to force the assignment, even if the organization of the target collector group is under migration.
- **Output Parameter:**
  - **ignoredCollectorGroupNames:** Specifies the list of collector groups already assigned to the policy.
- **Errors:**
  - Error code 400 Bad Request is returned if the given parameters do not match the expected format or values range.
  - Error code 500 Internal Server Error is returned for an unexpected error. In this case, contact Fortinet support.

For this API call, the **organization** parameter only supports the name of a specific organization. The value that you specify for the organization must match exactly.

Sample Request

https://ENSILOHOST/management-rest/playbooks-policies/assign-collector-group?policyName=playbook&collectorsGroupName=myGroup

Sample Response

```
{
"ignoredCollectorGroupNames": [
"aa"
]
}
```

list-policies (GET)

This API call outputs a list of policies:

- **Input Parameters:**
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.
- **Output Parameters:**
  - **id:** Specifies the policy ID.

- **name:** Specifies the name of the policy.
- **operationMode:** Specifies the policy mode.
- **organization:** Specifies the organization for the policy.
- **description:** Provides a description of the policy.
- **collectorGroups:** Specifies the list of collector group names to which the policy applies.
- **classificationActions:** Specifies the list of actions for each classification.

Sample Request

https://ENSILOHOST/management-rest/playbooks-policies/list-policies

Sample Response


```
[
{
"id": 190,
"name": "Default Playbook",
"operationMode": "Simulation",
"organization": "Default",
"description": "Playbooks allows you to orchestrate your security decisions based
on collateral events knowledge and propagate it throughout your organization
efficiently and automatically. Automation of the incident response process means
that you can save time and money with Fortinet, which will perform the operations
automatically for you",
"collectorGroups": [
"High Security Collector Group",
"Default Collector Group",
"emulation"
],
"classificationActions": {
"ClassificationMalicious": [
"OpenTicket",
"CleanPersistenceData",
"TerminateProcess",
"SendSyslogNotification",
"IsolateDevice",
"SendMailNotification"
],
"ClassificationProbablyGood": [
"OpenTicket",
"SendSyslogNotification",
"SendMailNotification"
],
"ClassificationInconclusive": [
"OpenTicket",
],
"ClassificationPup": [

],
"ClassificationProbablyMalicious": [
"OpenTicket",
"SendSyslogNotification",
"IsolateDevice",
```

```
"SendMailNotification"
]
}
}
]
```

map-connectors-to-actions (PUT)

This API call assigns external systems connectors to playbook actions. These assignments determine the external systems on which the playbook action is automatically performed once an event is triggered. This API is supported for version 5.0.3.334 and above.

- **Input Parameters:**
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match the organization exactly.
- **Body Input Parameters:**
  - **policyName:** Specifies playbook policy name.
  - **customActionsToConnectorsMaps:** Specifies a list that maps between user-customized actions and connectors.
    - **actionName:** Specifies the name of the custom action. This is only applicable to actions that are associated with external systems' connectors.
    - **Connectors:** Specifies the list of connectors with which the action is performed. Missing connectors are unmapped for the specified action. An empty list deselects all connectors.
  - **fortinetActionsToConnectorsMaps:** Specifies a list that maps between out-of-the-box actions and connectors.
    - **actionName:** Specifies the name of the out-of-the-box action. This is only applicable to actions that are associated with external systems' connectors.
    - **Connectors:** Specifies the list of connectors with which the action is performed. Missing connectors are unmapped for the specified action. An empty list deselects all connectors.
- **Output Parameters:**
  - **policyName:** Specifies the playbook policy name.
  - **actionsToConnectorsMap:** Specifies the list of modified actions with the associated connector of each resulting from a change. This parameter holds the updated mapping between actions and connectors.

Sample Request

https://ENSILOHOST/management-rest/playbooks-policies/map-connectors-to-actions?organization=demo

Sample Body

```
{
"fortinetActionsToConnectorsMaps": [
    {
    "actionName": "Isolate device with NAC",
    "connectors": [
        "MyNACName"
        ]
    }
```

```
],
"policyName": "Default Playbook"
}
```

Sample Response

```
{
    "policyName": "Default Playbook",
    "actionsToConnectorsMap": {
        "Isolate device with NAC": [
            "MyNACName"
        ]
    }
}
```

set-action-classification (PUT)

This API call sets the event classification to which the automatic incident response action applies. This API is supported for version 5.0.3.334 and above.

- **Input Parameters:**
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match the organization exactly.
- **Body Input Parameters:**
  - **policyName:** Specifies the playbook policy name.
  - **customActionsToClassificationMaps:** Specifies a list that maps between user-customized actions and event classifications.
    - **actionName:** Specifies the name of the custom action.
    - **classifications:** Specifies the list of event classifications upon which the action will automatically trigger. Missing classifications are disabled for the specified action. Valid values are: Malicious, Suspicious, PUP, Inconclusive and Likely Safe.
  - **fortinetActionsToClassificationMaps:** Specifies a list that maps between out-of-the-box actions and event classifications.
    - **actionName:** Specifies the name of the out-of-the-box action.
    - **classifications:** Specifies the list of event classifications upon which the action automatically triggers. Missing classifications are disabled for the specified action. Valid values are: Malicious, Suspicious, PUP, Inconclusive and Likely Safe.
- **Output Parameters:**
  - **policyName:** Specifies the playbook policy name.
  - **actionsToClassificationsMap:** Specifies the list of all actions with the associated classifications following the change.

Sample Request

https://104.199.102.198/management-rest/playbooks-policies/set-action-classification?organization=demo

Sample Body


```
{
"fortinetActionsToClassificationMaps": [
{
"actionName": "Open ticket",
"classifications": [
"Malicious"
]
}
],
"policyName": "Default Playbook"
}
```

Threat Hunting

search (POST)

This API call enables you to search for Indicators of Compromise (IOCs) and malware among the activity data that is collected and stored on the Repository server. Searches can be based on various attributes of files, registry keys/values, networks, processes, event log and activity event types. This API call is supported from version 5.0 and above.

- **Body Input Parameters:**
  - **organization:** Specifies the organization name in multi-tenant environments.
  - **category:** Specifies the category name, either: **Process**, **File**, **Registry**, **Network** or **Event Log**. **All** is the default value.
  - **devices:** Specifies the list of devices on which the events have occurred.
  - **time:** Specifies the time period of the events, either**: lastHour**, **last12hours**, **last24hours**, **last7days**, **last30days** or **custom**. The default value is **lastHour**.
  - **fromTime:** Specifies the starting (from) creation time of the events using the yyyy-MM-dd HH:mm:ss format. When using this parameter, the **time** parameter must be set to **custom**.
  - **toTime:** Specifies the ending (to) creation time of events. Specify the date using the yyyy-MM-dd HH:mm:ss format. When using this parameter, the **time** parameter must be set to **custom**.
  - **filters:** Specifies the filters to add to the query. Each holds the following parameters:
    - **fieldName:** Specifies the filter field name.
    - **includeValues:** Specifies whether the values list should be included or excluded from the query (**true** to include, **false** to exclude).
    - **values:** Specifies the list of values to be included or excluded from the query.
  - **itemsPerPage:** Specifies an integer to be used for paging that indicates the number of activity events to retrieve for the current page. The default is 100.
  - **pageNumber:** An integer used for paging that indicates the required page number.
  - **query:** Specifies a query with Lucene syntax.
  - **sorting:** Specifies the list of sorting objects. Each holds the following parameters:
    - **field:** Specifies the field by which to sort.
    - **order:** Specifies either 1 for ascending or -1 for descending.
    - **priority:** Specifies the level of sorting. Sorting can be done based on multiple fields, starting with priority 0 and then internal sorting 1, 2, 3 and so on.

Sample Request

https://ENSILOHOST/management-rest/threat-hunting/search

Sample Body

```
{
    "time": "lastHour",
    "category": "File",
    "itemsPerPage": 1,
    "devices": ["WIN1064"],
    "filters": [{
      "fieldName": "Type",
      "includeValues": true,
      "values": ["File Create", "File Delete"]
    }],
    "sorting": [{
      "field": "Type",
      "order": 1,
      "priority": 0
    }]
```

```
}
```

Sample Response


```
[
    {
        "SaveDate": 1613056377487,
        "Category": "File",
        "Device": {
            "KernelVersion": "10.0.18362 build 1316",
            "OS": "Windows NT",
            "CollectorId": 34605,
            "OSType": "Windows",
            "OSVersion": "10.0.18362 build 1316",
            "OrganizationId": 1,
            "CollectorVersion": "5.0.1.146",
            "InternalIp": [
                "10.51.121.111",
                "fe80::9558:4900:3715:e95d"
            ],
            "Name": "WIN1064"
        },
        "Time": 1613056374042,
        "Sequence": 13880,
        "Source": {
            "Process": {
                "CommandLine": "-host -hostId=78942014 -securityCookie=2460 -
initParameters=",
                "User": {
                    "Username": "Local System",
                    "UserId": "S-1-5-18"
                },
                "IntegrityLevel": "System",
                "CreationTime": 1613056369675,
                "ApplicationInfo": {
                    "CompanyName": "AO Kaspersky Lab",
                    "ProductName": "Kaspersky Anti-Virus",
                    "ProductVersion": "21.2.16.590"
                },
                "PID": 20864,
                "SessionID": 0,
                "File": {
                    "Ext": "exe",
                    "Path": "Program Files (x86)\\Kaspersky Lab\\Kaspersky Free 21.
2\\avp.exe",
                    "MountPoint": "C:",
                    "Type": "PE Executable",
                    "Owner": {
                        "Username": "Local System",
                        "UserId": "S-1-5-18"
                    },
                    "VolumeType": "Local",
                    "CreationTime": 1603350798000,
                    "ModificationTime": 1606231772696,
                    "OriginalDrive": "\\Device\\HarddiskVolume2\\",
                    "DownloadData": {},
                    "StaticFileData": {
                        "SHA1Hash": "5A4CCEEEA89F91ABFBFD15A98BF83DF2C6EB3D02",
                        "SigningInfo": {
                            "IsSigned": true,
```

```
                            "Signatures": [
                                {
                                    "SignedBy": "Kaspersky Lab JSC",
                                    "IsSignatureTimeValid": true,
                                    "Thumbprint": "D8322A553A0E35D5E25862BF3CF6BE96
C262E28D",
                                    "IsPrimary": true,
                                    "IsSignatureExpired": false,
                                    "IssuedBy": "DigiCert High Assurance Code Signi
ng CA-1",
                                    "IsValid": true
                                }
                            ]
                        },
                        "Size": 381928,
                        "Reputation": {
                            "Certainty": 30,
                            "Reputation": "ReputationSuspicious"
                        },
                        "ExecutableFormatData": {
                            "CompanyName": "AO Kaspersky Lab",
                            "FileDescription": "Kaspersky Anti-Virus",
                            "Architecture": "32-bit",
                            "ProductName": "Kaspersky Anti-Virus",
                            "FileVersion": "21.2.16.590",
                            "ProductVersion": "21.2.16.590"
                        },
                        "MachineLearning": {
                            "Score": 19,
                            "ModelVersion": 2
                        }
                    },
                    "Name": "avp.exe"
                },
                "ParentProcess": {
                    "Path": "\\Device\\HarddiskVolume2\\Program Files (x86)\\Kasper
sky Lab\\Kaspersky Free 21.2\\avp.exe",
                    "CreationTime": 1610934165773,
                    "PID": 2460
                },
                "TID": 20240,
                "Name": "avp.exe"
            }
        },
        "rowId": "4ec811be5882204d2ed751dfaf682b3c524390b4c826be3adecec678c42a2a0d"
,
        "TimeZone": -480,
        "Type": "File Create",
        "Target": {
            "File": {
                "Ext": "2\\Bases\\KSN\\temp",
```

```
                "Path": "ProgramData\\Kaspersky Lab\\AVP21.2\\Bases\\KSN\\temp",
                "AdditionalData": {
                    "Status": "0x00000000"
                },
                "Owner": {
                    "Username": "Administrators",
                    "UserId": "S-1-5-32-544"
                },
                "VolumeType": "Local",
                "CreationTime": 1613056374042,
                "ModificationTime": 1613056374042,
                "OriginalDrive": "\\Device\\HarddiskVolume2\\",
                "DownloadData": {},
                "Name": "temp"
            }
        },
        "TimeFromBoot": 2122253640,
        "EventProcessTime": 1613056377487,
        "ID": "4ec811be5882204d2ed751dfaf682b3c524390b4c826be3adecec678c42a2a0d"
    }
]
```


counts (POST)

This API call outputs the total count of activity events for each Threat Hunting category. This API is supported from version 5.0 and above.

- **Body Input Parameters:**
  - **organization:** Specifies the organization name in multi-tenant environments.
  - **category:** Specifies the category name, either: **Process**, **File**, **Registry**, **Network** or **Event Log**. All is the default value.
  - **devices:** Specifies the list of devices on which the events have occurred.
  - **time:** Specifies the time period of the events, either: **lastHour**, **last12hours**, **last24hours**, **last7days**, **last30days** or **custom**. The default value is **lastHour**.
  - **fromTime:** Specifies the starting (from) creation time of the events using the yyyy-MM-dd HH:mm:ss format. When using this parameter, the **time** parameter must be set to **custom**.
  - **toTime:** Specifies the ending (to) creation time. Specify the date using the yyyy-MM-dd HH:mm:ss format. When using this parameter, the **time** parameter must be set to **custom**.
  - **Filters:** Specifies the filters to add to the query. Each holds the following parameters
    - **fieldName:** Specifies the filter field name.
    - **includeValues:** Specifies whether the values list should be included or excluded from the query. Use **true** to include and **false** to exclude.
    - **values:** Specifies the list of values that will be included or excluded from the query.
  - **query:** Specifies a query with Lucene syntax.
  - **sorting:** Specifies the list of sorting objects. Each holds the following parameters:
    - **field:** Specifies the field by which to sort.
    - **order:** Specifies either 1 for ascending or -1 for descending.
    - **priority:** Specifies the level of sorting. Sorting can be done based on multiple fields, starting with priority 0 and then internal sorting 1, 2, 3 and so on.

Sample Request

https://ENSILOHOST/management-rest/threat-hunting/counts

Sample Body

```
{
    "time": "lastHour",
    "category": "File",
    "itemsPerPage": 1,
    "devices": ["WIN1064"],
    "filters": [{
      "fieldName": "Type",
      "includeValues": true,
      "values": ["File Create", "File Delete"]
    }],
    "sorting": [{
      "field": "Type",
      "order": 1,
      "priority": 0
    }]
}
```

Sample Response

```
{
  "all": 12732,
  "File": 12732
}
```

facets (POST)

This API call retrieves up to 100 activity events for every Threat Hunting facet item. This API is supported from version 5.0 and above.

- **Body Input Parameters:**
  - **organization:** Specifies the organization name in multi-tenant environments.
  - **category:** Specifies the category name, either: **Process**, **File**, **Registry**, **Network** or **Event** Log. **All** is the default value.
  - **devices:** Specifies the list of devices on which the events have occurred.
  - **time:** Specifies the time period of the events, either**: lastHour**, **last12hours**, **last24hours**, **last7days**, **last30days** or **custom**. The default value is **lastHour**.
  - **fromTime:** Specifies the starting (from) creation time of the events using the yyyy-MM-dd HH:mm:ss format. When using this parameter, the **time** parameter must be set to **custom**.
  - **toTime:** Specifies the ending (to) creation time. Specify the date using the yyyy-MM-dd HH:mm:ss format. When using this parameter, the **time** parameter must be set to **custom**.
  - **filters:** Specifies the filters to add to the query. Each holds the following parameters:
    - **fieldName:** Specifies the filter field name.
    - **includeValues:** Specifies whether the values list should be included or excluded from the query.
    - **values:** Specifies the list of values that will be included or excluded from the query.
  - **itemsPerPage:** An integer used for paging that indicates the number of activity events to retrieve for the current page. The default is 100.
  - **pageNumber:** An integer used for paging that specifies the required page number.
  - **query:** Specifies a query with Lucene syntax.
  - **sorting:** Specifies the list of sorting objects. Each holds the following parameters:
    - **field:** Specifies the field by which to sort.
    - **order:** Specifies either 1 for ascending or -1 for descending.
    - **priority:** Specifies the level of sorting. Sorting can be done based on multiple fields, starting with priority 0 and then internal sorting 1, 2, 3 and so on.
  - **facets:**

- **fieldname:** Specifies the facet name.
- **order:** Specifies either 1 for ascending or -1 for descending.
- **numOfDisplayedItems**: Specifies the number of items to retrieve.

Sample Request

https://ENSILOHOST/management-rest/threat-hunting/facets

Sample Body

```
{
    "time": "lastHour",
    "category": "File",
    "itemsPerPage": 1,
    "devices": ["WIN1064"],
    "filters": [{
      "fieldName": "Type",
      "includeValues": true,
      "values": ["File Create", "File Delete"]
    }],
    "sorting": [{
      "field": "Type",
      "order": 1,
      "priority": 0
    }],
    "facets" : [{
        "fieldName" : "Type",
        "numOfDisplayedItems": 5,
        "order": 0
   }]
}
```

Sample Response

```
[
    {
        "identifier": "Type",
        "distinctValuesCount": 2,
        "total": 174,
        "distinctValuesCountExceeded": false,
        "hierarchyPath": "Type",
        "values": [
            {
                "name": "File Create",
                "count": 89
            },
            {
                "name": "File Delete",
                "count": 85
            }
        ]
    }
]
```

save-query (POST)

This API call saves or edits a Threat Hunting query. This API is supported from version 5.0.2 and above.

- **Input Parameters:**
  - **Id:** Specifies the query ID to edit (not required for creating a new query). For an 'All-Organization' query Id is not applicable and only queryToEdit should be used.
  - **queryToEdit:** Specifies the query name to edit (not required for creating a new query).
- **Body Input Parameters:**
  - **category:** Specifies the category name, which is either: **Process**, **File**, **Registry**, **Network** or **Event** Log. **All** is the default value.
  - **classification:** Specifies the classification of events that are triggered with this query. This field is only relevant when the **scheduled** property is set to **True**. Valid values are: **Malicious**, **Suspicious**, **Inconclusive**, **Likely Safe**, **PUP** or **Safe**.
  - **collectorNames:** Specifies the Collector names.
  - **Community:** A true/false parameter indicating whether the query is available to the entire FortiEDR Community. **False** by default.
  - **name:** Specifies the name of the saved query being saved.
  - **description:** Specifies a description of the saved query.
  - **forceSaving:** A true/false parameter indicating whether to force the save, even when there is a large quantity of query results.
  - **organization:** Specifies the name of a specific organization. The value that you specify here must be an exact match.
  - **query:** Specifies the Lucene-like search query.
  - **scheduled:** Specifies whether the query is scheduled. **False** by default.
  - **frequency:** Specifies the query frequency for the scheduled query. The scheduled property must be true.
  - **frequencyUnit:** Specifies the query frequency unit. The **scheduled** property must be **True**. Valid values: **Minutes**, **Hours**, **Week**, **Day** or **Month**.
  - **hour:** Specifies the hour of the day for the scheduled query. The value must be between 0 and 23. The properties **scheduled** and **frequencyUnit** must be **True** and **Day/Week/Month** respectively.
  - **dayOfMonth:** Specifies the day of the month for the scheduled query. The value must be between 1 and 28. The properties **scheduled** and **frequencyUnit** must be **True** and **Month** respectively.
  - **dayOfWeek:** Specifies the day of the week for the scheduled query. The value must be between 0 and 6. 0 is Sunday and 6 is Saturday. The properties **scheduled** and **frequencyUnit** must be **True** and **Week** respectively.
  - **state:** A true/false parameter indicating whether the query state is enabled. **True** by default.
  - **tagIds:** Specifies the query Tag IDs. Tag IDs can be obtained using the list-tags API.
  - **tagNames:** Specifies the query tag names.
  - **time:** Specifies the time period of the events, either**: lastHour**, **last12hours**, **last24hours** or **last7days**, **last30days** or **custom**.
  - **fromTime:** Specifies the starting (from) creation time of the events using the yyyy-MM-dd HH:mm:ss format. When using this parameter, the **time** parameter must be set to **custom**.
  - **toTime:** Specifies the ending (to) creation time. Specify the date using the yyyy-MM-dd HH:mm:ss format. When using this parameter, the **time** parameter must be set to **custom**.

Sample Request

https://ENSILOHOST/management-rest/threat-hunting/save-query

Sample Body


```
{
"category": "Process",
"collectorNames": [
"Benjamin-PC"
],
"community": false,
"description": "Track Ben's activity",
"forceSaving": false,
"name": "svchost created Ben",
"organization": "DEMO",
"query": "Type:(Process Creation) AND Source.Process.Name: (svchost.exe)",
"scheduled": false,
"state": false,
"tagNames": [
"tracking_6"
],
"time": "lastHour"
}
```


set-query-state (PUT)

This API call updates the state of scheduled saved queries. This API is supported from version 5.0.2 and above.

- **Input Parameters:**
  - **organization**: Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.
  - **source:** Specifies a list of query sources. Valid item values are: **User** or **Community**.
  - **queryIds:** Specifies the query IDs list. This is not applicable to an "All organizations" query where queryNames input parameter should be used instead.
  - **queryNames:** Specifies the query names list.
  - **state:** A true/false parameter indicating whether to set the queries state to enabled.
  - **markAll:** A true/false value specifying whether all queries should be marked with the same value as the **state** property indicates.

Sample Request

https://ENSILOHOST/management-rest/threat-hunting/set-query-state?source=User&queryNames=myQuery&organization=DEMO&scheduled=true&state=true

delete-saved-queries (DELETE)

This API call deletes saved queries. This API is supported from version 5.0.2 and above.

- **Input Parameters:**
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.
  - **source:** Specifies a list of query sources. Valid item values are: **User** or **Community**.
  - **queryIds:** Specifies the query IDs list. This is not applicable to an “All organizations” query where queryNames input parameter should be used instead.
  - **queryNames:** Specifies the query names list.
  - **scheduled:** A true/false value specifying whether the query is scheduled.
  - **deleteFromCommunity:** A true/false value specifying whether to delete the query from the FortiEDR community as well. Only valid when **Community** is the value in the **source** field (described above).
  - **deleteAll:** A true/false value specifying whether all queries should be deleted.

Sample Request

https://ENSILOHOST/management-rest/threat-hunting/delete-saved-queries?source=User&queryNames=mytest&organization=DEMO&scheduled=false

list-saved-queries (GET)

This API call lists saved queries. This API is supported from version 5.0.2 and above.

- **Input Parameters:**
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.
  - **source:** Specifies a list of query sources. Valid item values are: **User** or **Community**.
  - **scheduled:** A true/false value specifying whether the query is scheduled.

Sample Request

https://ENSILOHOST/management-rest/threat-hunting/list-saved-queries?source=User&scheduled=false

create-or-edit-tag (POST)

This API call creates or edits a new tag for saved Threat Hunting queries. This API is supported from version 5.0.2 and above.

- **Body Input Parameters:**
  - **organization:** Specifies the organization. It is used only when editing an existing tag. When the API is being used for creating a new tag, the organization is determined by the organization to which the API user belongs.

    For editing, the value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.
  - **newTagName: (Mandatory)** Specifies tag name.
  - **tagID:** Specifies the ID of the tag to be edited. You can get the ID with list-tags API.
  - **tagName:** Specifies the name of the tag to be edited. It can be used instead of tagID.

Sample Request

```
https://ENSILOHOST/management-rest/threat-hunting/create-or-edit-tag
```

Sample Body

```
{
"newTagName": "badActorName"
}
```

delete-tags (DELETE)

This API call deletes saved queries tags. This API is supported from version 5.0.2 and above.

- **Input Parameters:**
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.
  - **tagIds:** Specifies a list of tag IDs to be deleted. Tag IDs can be obtained with list-tags API.
  - **tagNames:** Specifies a list of tag names to be deleted.

Sample Request

```
https://ENSILOHOST/management-rest/threat-hunting/delete-tags?tagNames=badActorName
```

list-tags (GET)

This API call lists saved queries tags. This API is supported from version 5.0.2 and above.

- **Input Parameters:**
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.

Sample Request

https://ENSILOHOST/management-rest/threat-hunting/list-tags

Threat Hunting Settings

threat-hunting-profile-clone (POST)

This API call clones a Threat Hunting profile.

Input Parameters:

- **organization:** Specifies the name of a specific organization. The value specified here must match exactly.
- **existingProfileName:** Specifies the name of the existing profile to be cloned.
- **cloneProfileName:** Specifies the name of the cloned Threat Hunting profile.

Sample Request

https://ENSILOHOST/management-rest/threat-hunting-settings/threat-hunting-profile-clone?organization=ensilofordev&existingProfileName=Inventory Profile&cloneProfileName=NewInventoryProfile

threat-hunting-profile (POST)

This API call edits an existing Threat Hunting profile based on its name and organization.

- **Body Input Parameters:**
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
  - **name:** Specifies a name to be used to identify this Threat Hunting profile (mandatory).
  - **newname:** Specifies a new name for this profile.
  - **associatedCollectorGroupIds:** Specifies the IDs of collector groups to be associated with this profile. collector group IDs can be retrieved using list-collector-groups API call. (Required)
  - **threatHuntingCategoryList:** Specifies the list of categories and event types to be enabled under the profile.
    - **name:** Specifies the Threat Hunting category. Use the threat-hunting-metadata API call to get the list of valid Categories. For example: **Process**.
    - **enabled:** Specifies whether the category is set to enabled (collect data), either **True** or **False**.
    - **eventTypes:** Specifies the event types under this category for which data collection is to be enabled. For example: Process Termination or Process Creation.
- **Output parameters:**
  - **Name:** Specifies the name of this Threat Hunting profile.
  - **associatedCollectorGroupIds:** Specified the Ids of collector groups that are associated with this profile.
  - **Immutable:** When **True**, this profile comes out of the box and cannot be changed.
  - **threatHuntingCategoryList:** Specifies the list of categories and event types that are enabled under the profile.
    - **name:** Specifies the Threat Hunting category.
    - **enabled:** Specifies whether the category is set to enabled (collect data), either **True** or **False**.
    - **eventTypes:** Specifies the event types under this category for which data collection is enabled.

Sample Request

https://ENSILOHOST/management-rest/threat-hunting-settings/threat-hunting-profile?organization=ensilofordev&name=XDR Profile Einat

Sample Body

```
{
      "organization": "ensilofordev",
      "name": "XDR Profile Einat",
      "newName" : "XDR Profile Einat Sample",
    "associatedCollectorGroupIds" : [ ],
    "threatHuntingCategoryList" : [ {
```

```
      "name" : "Process",
      "enabled" : true,
      "eventTypes" : [ "Process Creation" ]
    }, {
      "name" : "File",
      "enabled" : false,
      "eventTypes" : [ "File Create" ]
    }, {
      "name" : "Registry",
      "enabled" : false,
      "eventTypes" : [ ]
    }, {
      "name" : "Network",
      "enabled" : true,
      "eventTypes" : [ "Socket Connect" ]
    }, {
      "name" : "Event Log",
      "enabled" : false,
      "eventTypes" : [ ]
    }, {
      "name" : "Inventory Scan",
      "enabled" : true,
      "eventTypes" : [ "File Detected" ]
    } ]
}
```

assign-collector-groups (POST)

This API call updates the assigned collector groups for a Threat Hunting profile and returns the updated list of assigned collector groups. This API is supported from version 5.0.3 and above.

- **Body Input Parameters:**
  - **organization:** Specifies the name of a specific organization. This value must match exactly.
  - **name:** Specifies the name that is used to identify the Threat Hunting profile.
  - **associatedCollectorGroupIds:** List of collector groups IDs to be assigned to the specified Threat Hunting profile. For example: [1,2,3].

Sample Request

https://ENSILOHOST/management-rest/threat-hunting-settings/assign-collector-groups

Sample Body

```
{
"associatedCollectorGroupIds": [
23151479
],
"name": "No Collection",
"organization": "myOrganization"
}
```

threat-hunting-profile (DELETE)

This API call deletes a Threat Hunting profile by its name. Out of the box profiles cannot be deleted.

- **Input Parameters:**
  - **organization**: Specifies the name of a specific organization. The value specified here must match exactly.
  - **name:** Specifies the name that is used to identify the Threat Hunting profile.

Sample Request

https://ENSILOHOST/management-rest/threat-hunting-settings/threat-hunting-profile?

threat-hunting-profile (GET)

This API call outputs a list of the Threat Hunting data collection profiles that are in use for different collector groups in the organization.

- **Input Parameters:**
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.

Sample Request

https://ENSILOHOST/management-rest/threat-hunting-settings/threat-hunting-profile

threat-hunting-metadata (GET)

This API call lists the metadata and available configurations options of Threat Hunting data collection profiles. When creating/modifying a Threat Hunting profile, use the response of this API as a guide for the valid categories and event type values.

Sample Request:

https://ENSILOHOST/management-rest/threat-hunting-settings/threat-hunting-metadata

Sample Response:


```
[
        {
            "categoryName": "Inventory Scan",
            "eventTypes": [
                "File Detected"
            ]
        },
        {
            "categoryName": "Process",
            "eventTypes": [
                "Process Termination",
                "Process Creation",
                "Process Start",
                "Thread Created",
                "Executable Loaded",
                "Driver Loaded",
                "Library Loaded"
            ]
        },
        {
```

```
            "categoryName": "File",
            "eventTypes": [
                "File Create",
                "File Write",
                "File Read",
                "File Rename",
                "File Delete"
            ]
        },
        {
            "categoryName": "Network",
            "eventTypes": [
                "Socket Connect",
                "Socket Bind",
                "Socket Listen",
                "Socket Close",
                "Socket Accept"
            ]
        },
        {
            "categoryName": "Registry",
            "eventTypes": [
                "Key Created",
                "Key Deleted",
                "Key Renamed",
                "Value Created",
                "Value Read",
                "Value Deleted",
                "Value Set"
            ]
        },
        {
            "categoryName": "Event Log",
            "eventTypes": [
                "Log Entry Created"
            ]
        }
    ]
```

Exclusions

exclusions (POST)

This API call creates one or more exclusions. The exclusion list to be associated with this newly created exclusion must already be defined. This API is supported from version 5.0 and above.

- **Body Input Parameters:**
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
  - **exclusionListName:** Specifies the name of a list with which newly created exclusions will be associated. This field is mandatory.
  - **Exclusions:** Specifies the **list** of exclusions definitions to be created, each with the following fields:
    - **attributes:** Specifies the list of exclusion attributes defining this exclusion. Use the following API to get a list of possible values: /exclusions/exclusions-metadata. Attributes consist of the following fields:
      - **type:** Specifies the attribute type, either **Source** or **Target**.
      - **name:** Specifies the attribute name.
      - **secondaryValue:** Specifies the secondary property identifying the attribute. Used in special cases like with the Signer attribute.
      - **value:** Specifies the attribute value.
    - **comments:** Specifies a comment to be added to the exclusion.
    - **enabled:** Specifies the exclusion enabled/disabled status.
    - **eventTypes:** Specifies the list of activity event types to be covered by this exclusion.
    - **operatingSystems:** Specifies the operating systems on which the exclusion applies.

Sample Request

https://ENSILOHOST/management-rest/exclusions/exclusion

Sample Body

```
{
   "exclusionListName":"Rest List53",
   "exclusions":[
      {
         "attributes":[
            {
               "name":"Signer",
               "type":"Source",
               "secondaryValue": "SignerName",
               "value":"exact signer name"
            }
         ],
         "comments":"comments example",
         "enabled":true,
         "eventTypes":[
            "Process Termination",
            "Process Creation"
         ],
         "operatingSystems":[
            "Windows"
         ]
      }
   ],
```

```
   "organization":"Default"
}
Sample Response
[
    {
        "enabled": true,
        "attributes": [
            {
                "name": "Signer",
                "value": "exact signer name",
                "type": "Source",
                "secondaryValue": "SignerName"
            }
        ],
        "eventTypes": [
            "Process Termination",
            "Process Creation"
        ],
        "operatingSystems": [
            "Windows"
        ],
        "comments": "comments example",
        "id": 23699,
        "lastDateModified": "Wed Feb 03 21:22:11 IST 2021",
        "lastUserModifier": "admin"
    }
]
```

exclusions (PUT)

This API call edits one or more existing exclusions by exclusion IDs. This API is supported from version 5.0 and above.

Body Input Parameters:

- **Exclusions:** List of exclusions definitions to be edited, each with the following fields:
  - **exclusionListName:** Specifies the name of a list with which the exclusions being edited are associated**.** This field is mandatory.
  - **Exclusions:** Specifies the **list** of exclusions definitions to be created, each with the following fields:
    - **exclusionId:** Specifies the exclusion's ID.
    - **attributes:** Specifies the list of exclusion attributes defining this exclusion. Use the following API to get a list of possible values: /exclusions/exclusions-metadata. Attributes consist of the following fields:
      - **type:** Specifies the attribute type, either **Source** or **Target**.
      - **name:** Specifies the attribute name.
      - **secondaryValue:** Specifies the secondary property identifying the attribute. Used in special cases like with the Signer attribute.
      - **value:** Specifies the attribute value.
    - **comments:** Specifies a comment to be added to the exclusion.
    - **enabled:** Specifies the exclusion enabled/disabled status.
    - **eventTypes:** Specifies the list of activity event types to be covered by this exclusion.
    - **operatingSystems:** Specifies the operating systems on which the exclusion applies.

Sample Request

https://ENSILOHOST/management-rest/exclusions/exclusion

Sample Body


```
{
    "exclusionListName": "Rest List53",
    "exclusions": [
        {
            "enabled": true,
            "attributes": [
                {
                    "name": "Signer",
                    "value": "exact signer name 2",
                    "type": "Source",
                    "secondaryValue": "SignerName"
                }
            ],
            "eventTypes": [
                "Process Termination",
                "Process Creation"
            ],
            "operatingSystems": [
                "Windows"
            ],
            "comments": "comments example 2",
            "exclusionId": 23699
        }
    ],
    "organization": "Default"
}
```


Sample Response


```
[
    {
        "enabled": true,
        "attributes": [
            {
                "name": "Signer",
                "value": "exact signer name 2",
                "type": "Source",
                "secondaryValue": "SignerName"
            }
        ],
        "eventTypes": [
            "Process Termination",
            "Process Creation"
        ],
        "operatingSystems": [
            "Windows"
        ],
        "comments": "comments example 2",
        "id": 23699,
        "lastDateModified": "Wed Feb 03 21:25:38 IST 2021",
        "lastUserModifier": "admin"
```

```
    }
]
```

exclusions (DELETE)

This API call deletes one or more exclusions by ID. This API is supported from version 5.0 and above.

Body Input Parameters:

- **organization:** Specifies the name of a specific organization. The value specified here must match exactly.
- **exclusionIds:** List of exclusion IDs for deletion.

Sample Request

https://ENSILOHOST/management-rest/exclusions/exclusion

Sample Body

```
{
  "exclusionIds": [
    0
  ],
  "organization": "DEMO"
}
```

exclusions-list (GET)

This API call outputs a list of exclusion lists and the associated exclusions within. This API is supported from version 5.0 and above.

Input Parameters:

- **organization:** Specifies the name of a specific organization. The value specified here must match exactly.

Sample Request

https://ENSILOHOST/management-rest/exclusions/exclusions-list?ensilofordev

Sample Response


```
[
 {
        "id": 4535435,
        "name": "test",
        "exclusions": [
            {
                "enabled": false,
                "attributes": [
                    {
                        "name": "Path",
                        "value": "\a\b C:\\Program Files (x86)\\Adobe\\Acrobat Reader DC\\",
                        "type": "Source"
                    }
                ],
                "eventTypes": [
                    "Process Creation"
                ],
                "operatingSystems": [
                    "Windows"
                ],
                "comments": "whitelist AR",
                "id": 4716896,
                "lastDateModified": "Mon Mar 22 10:52:35 EDT 2021",
                "lastUserModifier": "Einat"
            }
        ],
        "associatedCollectorGroups": [],
        "defaultExclusionList": false,
        "immutable": false
    }
]
```


exclusions-list (POST)

This API call creates an exclusions list. This API is supported from version 5.0 and above.

Body Input Parameters:

- **organization:** Specifies the name of a specific organization. The value specified here must match exactly.
- **collectorGroupIds:** Specifies the list of collector group IDs to be associated with this exclusion list. These IDs can be retrieved using list-collector-groups API.
- **name:** Exclusion list name.

Sample Request

https://ENSILOHOST/management-rest/exclusions/exclusions-list

Sample Body

```
{
  "collectorGroupIds": [
    27929
  ],
  "name": "myNewExclusionList",
  "organization": "ensilofordev"
}
```

Sample Response

```
{
    "id": 4717030,
    "name": "myNewExclusionList",
    "exclusions": [],
    "associatedCollectorGroups": [
        {
            "name": "philip",
            "numberOfCollectors": 1,
            "id": 27929
        }
    ],
    "defaultExclusionList": false,
    "immutable": false
}
```

exclusions-list (PUT)

This API call updates an exclusions list. This API is supported from version 5.0 and above.

Body Input Parameters:

- **organization:** Specifies the name of a specific organization. The value specified here must match exactly.
- **listName:** Specifies the exclusion list name.
- **collectorGroupIds:** The list of collector group IDs to be associated with this exclusion list. These IDs can be retrieved using the list-collector-groups API.
- **newName:** Specifies the exclusion list's new name.

Sample Request

https://ENSILOHOST/management-rest/exclusions/exclusions-list

Sample Body

```
{
  "collectorGroupIds": [
    27929
  ],
  "listName": "test",
  "organization": "ensilofordev",
  "newName": "newtest"
}
```

Sample Response


```
{
    "id": 4535435,
    "name": "newtest",
    "exclusions": [],
    "associatedCollectorGroups": [
        {
            "name": "philip",
            "numberOfCollectors": 1,
            "id": 27929
        }
    ],
    "defaultExclusionList": false,
    "immutable": false
}
```


exclusions-list (DELETE)

This API deletes an exclusions list with all exclusions in it. This API is supported from version 5.0 and above.

Input Parameters:

- **organization:** Specifies the name of a specific organization. The value specified here must match exactly.
- **listName:** Specifies the exclusion list name.
- **Output Parameters –** None.

  Response code 200 indicates a successful operation.

Sample Request

https://ENSILOHOST/management-rest/exclusions/exclusions-list?organization=ensilofordev&listName=newtest

exclusions-search (GET)

This API performs a free text search for exclusions. It returns each exclusion list that contains the specified string or that contains an exclusion with any field that contains it. This API is supported from version 5.0 and above.

Input Parameters:

- **organization:** Specifies the name of a specific organization. The value specified here must match exactly.
- **searchText:** a free text search string.

Sample Request

https://ENSILOHOST/management-rest/exclusions/exclusions-search?organization=ensilofordev&searchText=build

Sample Response


```
[
    {
        "id": 4417779,
        "name": "MyBuildServices",
        "exclusions": [],
        "associatedCollectorGroups": [],
        "defaultExclusionList": false,
        "immutable": false
    }
]
```

exclusions-metadata (GET)

This API call lists the metadata and available properties for exclusions configuration. When creating/modifying an exclusion, use the response of this API as a guide for the valid attribute names and values, and their corresponding activity event types. Every attribute corresponds to an activity event category (for example, the Filename attribute corresponds to the File category), and each category is a set of activity event types.

Sample Request

https://ENSILOHOST/management-rest/exclusions/exclusions-metadata

Sample Response


```
  "categories": [
    {
      "eventTypesNames": [
        "string"
      ],
      "name": "string"
    }
  ],
  "operatingSystems": [
    "string"
  ],
  "sourceAttributes": [
    {
      "description": "string",
      "inputType": "string",
      "name": "string",
      "options": [
        "string"
      ],
      "secondaryValue": "string",
      "supportedCategories": [
        "string"
      ]
    }
  ],
  "targetAttributes": [
    {
      "description": "string",
      "inputType": "string",
      "name": "string",
      "options": [
        "string"
      ],
      "secondaryValue": "string",
      "supportedCategories": [
        "string"
      ]
    }
  ]
}
```

Hash

search (GET) – Deprecated from V5.0

This API call is supported from version 2.6.4 and up to version 4.2. For versions V5.0 and above use Threat Hunting APIs:

This API call enables you to search a file hash among the current events, threat hunting repository and communicating applications that exist in the system.

- **Input Parameters:**
  - **fileHashes:** Specifies the list of hashes (separated by commas) that you want to search.
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.
- **Output Parameters –** Searches events, the threat hunting repository and communicating applications for a file hash (one or more):
  - **eventIds:** Specifies list of the event IDs.
  - **applications:** Specifies the list of the applications with the following fields:
    - **vendor:** Specifies a single value for the vendor name. By default, **strictMode** is false.
    - **product:** Specifies a single value for the product name. By default, **strictMode** is false.
    - **version:** Specifies a single value for the version name. By default, **strictMode** is false.
    - **processes:** Specifies the list of process names running alongside the products.
    - **firstConnectionTimeStart:** Retrieves products whose last connection time is greater than the value assigned to this date.

      Date Format: yyyy-MM-dd HH:mm:ss.
    - **lastConnectionTimeEnd:** Retrieves products whose last connection time is less than the value assigned to this date.

      Date Format: yyyy-MM-dd HH:mm:ss.
    - **organization:** The organization of the application.
  - **collectors:** Specifies the list of collectors that reported the product, in JSON format. Each collector holds the following parameters:
    - **device:** Specifies the device name.
    - **ip:** Specifies the device IP address.
    - **os:** Specifies the device operating system.
    - **lastSeen:** Specifies the date when the collector was last seen.
    - **collectorsGroupdecisions:** Specifies the list of communication control policies and their decisions for this specific product.
  - **seen:** A true/false parameter indicating whether events were read/unread by the user operating the API.
  - **handled:** A true/false parameter indicating whether events were handled/unhandled.
  - **statistics:** Specifies the application statistics.
  - **recommendation:** Specifies the recommendation of the application. Possible values are **Unknown**, **Known_bad**, **Assumed_bad**, **Contradiction**, **Assumed_good** or **Known_good**.

- **decisionv2:** Specifies the list communication control policies and their decisions and mode for this specific product with the following fields:
  - **policyName:** Specifies the policy name.
  - **PolicyMode:** Specifies the policy mode.
  - **decision:** Indicates the action.
- **threatsHunting:** Specifies the list of the applications with the following fields:
  - **deviceName:** Specifies the device name.
  - **fileName:** Specifies the file name.
  - **path:** Specifies the path

Integrations

create-connector (POST)

This API call creates a new connector for integration with external systems. Use the connectors-metadata API to get valid values for each connector. Custom connectors and actions are not supported by this API. This API is supported from version 5.0 and above.

- **Body Input Parameters:**
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
  - **type:** Specifies the type of connector to be used. For example, **NAC**.
  - **name:** Specifies a free text name to be used to identify this connector.
  - **enabled:** Specifies whether the connector is enabled or not: **True/False**.
  - **coreId:** Specifies the FortiEDR Core with JumpBox capabilities that enables communication with the external system.
  - **vendor:** Specifies the connector's vendor. For example: **FortiNAC**.
  - **host:** Specifies the IP or DNS address of the external system.
  - **port:** Specifies the port that is used for API communication with the external system.
  - **username:** Specifies the external system API user's username for authentication. If apiKey is used instead, then this field should be left empty.
  - **password:** Specifies the external system's API user's password for authentication. If apiKey is used instead, then this field should be left empty.
  - **apiKey:** Specifies the connector's API key for authentication. If username and passwords are used instead, then this field (apiKey) should be left empty.
  - **connectorActions:** Specifies the connector's actions' definition. Use connectors-metadata API for supported values.
    - **identifierName:** Specifies the action's identifier name.
    - **scriptName:** Specifies the action's script name. Action script must correspond the connector's vendor.
    - **actionProperties:** Specifies the action's property list, which is mandatory for some connector types.
      - **identifierName:** Specifies the property identifier name.
      - **value:** Specifies the property value for the specified identifier.

Sample Request

https://ENSILOHOST/management-rest/integrations/create-connector

Sample Body

```
{
  "apiKey": "abcdef12345",
  "connectorActions": [
    {
      "actionProperties": [
        ],
      "identifierName": "PbFabricActionNacIsolate",
      "scriptName": "PbFabricActionNacIsolate.py"
    }
  ],
  "coreId": "3927336",
  "enabled": false,
  "host": "10.51.1.1",
  "name": "MyNACName",
  "organization": "ensilofordev",
```

```
  "password":"",
  "port": 443,
  "type": "NAC",
  "username": "",
  "vendor": "FortiNAC"
}
```

delete-connector (DELETE)

This API call deletes a connector by type and name. This API is supported from version 5.0 and above.

- **Input Parameters:**
  - **organization:** Specifies the name of a specific organization. The value specified here must match exactly.
  - **connectorType:** Specifies the connector's type. For example: **NAC**.
  - **connectorName:** Specifies the connector's unique name. The value specified here is case sensitive.

Sample Request

https://ENSILOHOST/management-rest/integrations/delete-connector?organization=ensilofordev&connectorType=NAC&connectorName=MyNACName

list-connectors (GET)

This API call outputs lists all the connectors that are configured on FortiEDR and their configuration values. This API is supported from version 5.0 and above.

- **Input Parameters:**
  - **organization**: Specifies the name of a specific organization. The value specified here must match exactly.
  - **onlyValidConnectors**: Specifies whether to retrieve only enabled, non-failing connectors. Valid values ae : **True/False**.

Sample Request

https://ENSILOHOST/management-rest/integrations/list-connector

Sample Response

```
[ {
  "name" : "MyFW",
  "organization" : "ensilofordev",
  "enabled" : true,
  "host" : "1",
  "port" : "443",
  "type" : "Firewall",
  "username" : null,
  "password" : null,
  "apiKey" : "1",
  "coreId" : 3927336,
  "vendor" : "FortiGate",
  "connectorActions" : [ {
    "identifierName" : "PbFabricActionBlock",
    "scriptName" : "PbFabricActionBlock_Fortigate.py",
    "actionProperties" : [ {
      "identifierName" : "PolicyGroupName",
      "value" : "dd"
    } ]
  } ]
```

```
}, {
  "name" : "MyNAC",
  "organization" : "ensilofordev",
  "enabled" : true,
  "host" : "1",
  "port" : "443",
  "type" : "NAC",
  "username" : null,
  "password" : null,
  "apiKey" : "1",
  "coreId" : 3927336,
  "vendor" : "FortiNAC",
  "connectorActions" : [ {
    "identifierName" : "PbFabricActionNacIsolate",
    "scriptName" : "PbFabricActionNacIsolate.py",
    "actionProperties" : [ ]
  } ]
} ]
```


test-connector (GET)

This API call tests a connector by verifying connectivity to the integrated system, validating the authentication details and potentially other required configurations (connector-dependent). Custom connectors and actions are not supported by this API. This API is supported from version 5.0 and above.

Input Parameters:

- **organization:** Specifies the name of a specific organization. The value specified here must match exactly.
- **connectorType:** Specifies the connector's type. For example: **NAC**.
- **connectorName:** Specifies the connector's unique name. The value specified here is case sensitive.

Sample Request

https://ENSILOHOST/management-rest/integrations/test-connector?organization=ensilofordev&connectorType=NAC&connectorName=MyNACName

Sample Response:


```
{
    "connectorTestResult": "GENERAL_FAILURE",
    "testResultMessage": "Action failed. Try checking your connector configuration.
"
}
```


update-connector (PUT)

This API call edits a connector’s configuration, based on its type and name. Custom connectors and actions are not supported by this API. This API is supported from version 5.0 and above.

- **Body Input Parameters:**
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
  - **type:** Specifies the type of connector to be used. For example: **NAC**.
  - **name:** Specifies a name that is used to identify this connector.
  - **enabled:** Specifies whether the connector is enabled or not: **True/False**.

- **coreId:** Specifies the FortiEDR Core with JumpBox capabilities that enable communication with the external system.
- **vendor:** Specifies the connector's vendor. For example: **FortiNAC**.
- **host:** Specifies the IP or DNS address of the external system.
- **port:** Specifies the port that is used for API communication with the external system.
- **username:** Specifies the external system API user's username for authentication. If apiKey is used instead, then this field should be left empty.
- **password:** Specifies the external system's API user's password for authentication. If apiKey is used instead, then this field should be left empty.
- **apiKey:** Specifies the connector's API key for authentication. If username and passwords are used instead, then this field (apiKey) should be left empty.
- **connectorActions:** Specifies the connector's actions' definition. Use the connectors-metadata API for supported values.
  - **identifierName:** Specifies the action's identifier name.
  - **scriptName:** Specifies the action's script name. The action's script must correspond to the connector's vendor.
  - **actionProperties:** Specifies the action's property list (mandatory on some connector types).
    - **identifierName:** Specifies the property identifier name.
    - **value:** Specifies the property value for the specified identifier.

Sample Request

https://ENSILOHOST/management-rest/integrations/update-connector

Sample Body

```
{
  "apiKey": "abcdef12345",
  "connectorActions": [
    {
      "actionProperties": [
        ],
      "identifierName": "PbFabricActionNacIsolate",
      "scriptName": "PbFabricActionNacIsolate.py"
    }
  ],
  "coreId": "3927336",
  "enabled": true,
  "host": "10.51.1.1",
  "name": "MyNACName",
  "organization": "ensilofordev",
  "password":"",
  "port": 443,
  "type": "NAC",
  "username": "",
  "vendor": "FortiNAC"
}
```

connectors-metadata (GET)

This API call lists the metadata and available properties for a connector's configuration. When creating/modifying a connector, use the response of this API as a guide for the valid connector categories, types and actions. It also lists the available FortiEDR cores with JumpBox capabilities that enable integration with external systems and the onPremiseCores for backward compatibility (deprecated). This API is supported from version 5.0 and above.

Input Parameters:

- **organization:** Specifies the name of a specific organization. The value specified here must match exactly.

Sample Request

https://ENSILOHOST/management-rest/integrations/connectors-metadata

IoT

create-iot-group (POST)

This API call creates an IoT group:

- **Input Parameters:**
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
  - **name:** Specifies the IoT group name.

Sample Request

https://ENSILOHOST/management-rest/iot/create-iot-group?name=group1

delete-devices (DELETE)

This API call deletes IoT devices:

- **Input Parameters:**
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Indicates that the operation applies to all organizations. In this case, the same data is shared by all organizations.
  - **devicesIds:** Specifies the list of device IDs.
  - **devices:** Specifies the list of device names.
  - **iotGroups:** Specifies the list of collector group names and retrieves collectors under the given groups.
  - **iotGroupsIds:** Specifies the list of collector group IDs and retrieves collectors under the given groups.
  - **internalIps:** Specifies the list of IP values.
  - **macAddresses:** Specifies the list of MAC address values.
  - **categories:** Specifies the list of category values.
  - **models:** Specifies the list of model values.
  - **vendors:** Specifies the list of vendor values.
  - **locations:** Specifies the list of location values.
  - **firstSeenStart:** Retrieves the IoT devices that were first seen after the value assigned to this date.
    Date Format: yyyy-MM-dd HH:mm:ss.
  - **firstSeenEnd:** Retrieves the IoT devices that were first seen before the value assigned to this date.
    Date Format: yyyy-MM-dd HH:mm:ss.
  - **lastSeenStart:** Retrieves the IoT devices that were last seen after the value assigned to this date.
    Date Format: yyyy-MM-dd HH:mm:ss.
  - **lastSeenEnd:** Retrieves the IoT devices that were last seen before the value assigned to this date.
    Date Format: yyyy-MM-dd HH:mm:ss.
  - **showExpired:** Specifies whether to include IoT devices that have been disconnected for more than three days (sequentially) and are marked as Expired.

Sample Request

https://ENSILOHOST/management-rest/iot/delete-devices

export-iot-json (GET)

This API call outputs detailed information for an IoT device:

- **Input Parameters:**
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
  - **iotDeviceIds:** Specifies the list of device IDs.
- **Output Parameters:** This operation results in a file stream (binary data), which is a *.zip file.

Sample Request

https://ENSILOHOST/management-rest/iot/export-iot-json

list-iot-devices (GET)

This API call outputs a list of the IoT devices in the system. Use the input parameters to filter the list:

- **Input Parameters:**
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Specifies that the operation applies to all organizations. In this case, the same data is shared by all organizations.
  - **devicesIds:** Specifies the list of device IDs.
  - **devices:** Specifies the list of device names.
  - **iotGroups:** Specifies the list of collector group names and retrieves collectors under the given groups.
  - **iotGroupsIds:** Specifies the list of collector group IDs and retrieves collectors under the given groups.
  - **internalIps:** Specifies the list of IP values.
  - **macAddresses:** Specifies the list of MAC address values.
  - **categories:** Specifies the list of category values.
  - **models:** Specifies the list of model values.
  - **vendors:** Specifies the list of vendor values.
  - **locations:** Specifies the list of location values.
  - **firstSeenStart:** Retrieves IoT devices that were first seen after the value assigned to this date.
    Date Format: yyyy-MM-dd HH:mm:ss.
  - **firstSeenEnd:** Retrieves IoT devices that were first seen before the value assigned to this date.
    Date Format: yyyy-MM-dd HH:mm:ss.
  - **lastSeenStart:** Retrieves IoT devices that were last seen after the value assigned to this date.
    Date Format: yyyy-MM-dd HH:mm:ss.
  - **lastSeenEnd:** Retrieves IoT devices that were last seen before the value assigned to this date.
    Date Format: yyyy-MM-dd HH:mm:ss.
  - **showExpired:** Specifies whether or not to include IoT devices that have been disconnected for more than three days (sequentially) and are marked as Expired.

Sample Request

https://ENSILOHOST/management-rest/iot/list-iot-devices

Sample Response


```
[
  {
    "id": 95884,
    "deviceName": "ens-storsw",
    "category": "Network device",
    "userCategory": "Network device",
    "type": "Broadband router",
    "model": "Dell, IL, Linksys WRV200 wireless broadband router",
    "internalIp": "10.51.100.152",
    "location": null,
    "mac": "F4-8E-38-3F-94-A2",
    "isNew": false,
    "isExpired": false,
    "firstSeen": "2020-02-20 16:33",
    "lastSeen": "2020-03-04 15:00",
    "organization": "Default"
  }
]
```


list-iot-groups (GET)

This API call outputs the IoT device groups:

- **Input Parameters:**
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Specifies that the operation applies to all organizations. In this case, the same data is shared by all organizations.

Sample Request

https://ENSILOHOST/management-rest/iot/list-iot-groups

Sample Response


```
[
  {
    "id": 95866,
    "name": "Other",
    "organization": "Default"
  },
  {
    "id": 95867,
    "name": "Video Device",
    "organization": "Default"
  },
  {
    "id": 95973,
    "name": "Network device",
    "organization": "Default"
  },
]
```

move-iot-devices (PUT)

This API call moves IoT devices between groups:

- **Input Parameters:**
  - **organization:** Specifies the name of a specific organization. The value that you specify here must match exactly.
  - **iotDeviceIds:** Specifies the Array of IoT device IDs.
  - **targetIotGroup:** Specifies the IoT target group name.

Sample Request

https://ENSILOHOST/management-rest/iot/move-iot-devices

rescan-iot-device-details (PUT)

This API call refreshes the data of the specifies IoT device(s):

- **Input Parameters:**
  - **organization:** Specifies the organization. The value that you specify for this parameter indicates how the operation applies to an organization(s). Some parts of the Fortinet Endpoint Protection and Response Platform system have separate, non-shared data that is organization-specific. Other parts of the system have data that is shared by all organizations. The value that you specify for the organization parameter, as described below, determines to which organization(s) an operation applies:
    - **Exact organization name:** Specifies the name of a specific organization. The value that you specify here must match exactly.
    - **All organizations:** Specifies that the operation applies to all organizations. In this case, the same data is shared by all organizations.
  - **devicesIds:** Specifies the list of device IDs.
  - **devices:** Specifies the list of device names.
  - **iotGroups:** Specifies the list of collector group names and retrieves collectors under the given groups.
  - **iotGroupsIds:** Specifies the list of collector group ids and retrieves collectors under the given groups.
  - **internalIps:** Specifies the list of IP values.
  - **macAddresses:** Specifies the list of MAC address values.
  - **categories:** Specifies the list of category values.
  - **models:** Specifies the list of model values.
  - **vendors:** Specifies the list of vendor values.
  - **locations:** Specifies the list of location values.
  - **firstSeenStart:** Retrieves IoT devices that were first seen after the value assigned to this date.
    Date Format: yyyy-MM-dd HH:mm:ss.
  - **firstSeenEnd:** Retrieves IoT devices that were first seen before the value assigned to this date.
    Date Format: yyyy-MM-dd HH:mm:ss.
  - **lastSeenStart:** Retrieves IoT devices that were last seen after the value assigned to this date.
    Date Format: yyyy-MM-dd HH:mm:ss.
  - **lastSeenEnd:** Retrieves IoT devices that were last seen before the value assigned to this date.
    Date Format: yyyy-MM-dd HH:mm:ss.
  - **showExpired:** Specifies whether or not to include IoT devices that have been disconnected for more than three days (sequentially) and are marked as Expired.

Sample Request

https://ENSILOHOST/management-rest/iot/rescan-iot-device-details