# Integration API Guide

FortiSIEM 6.7.5
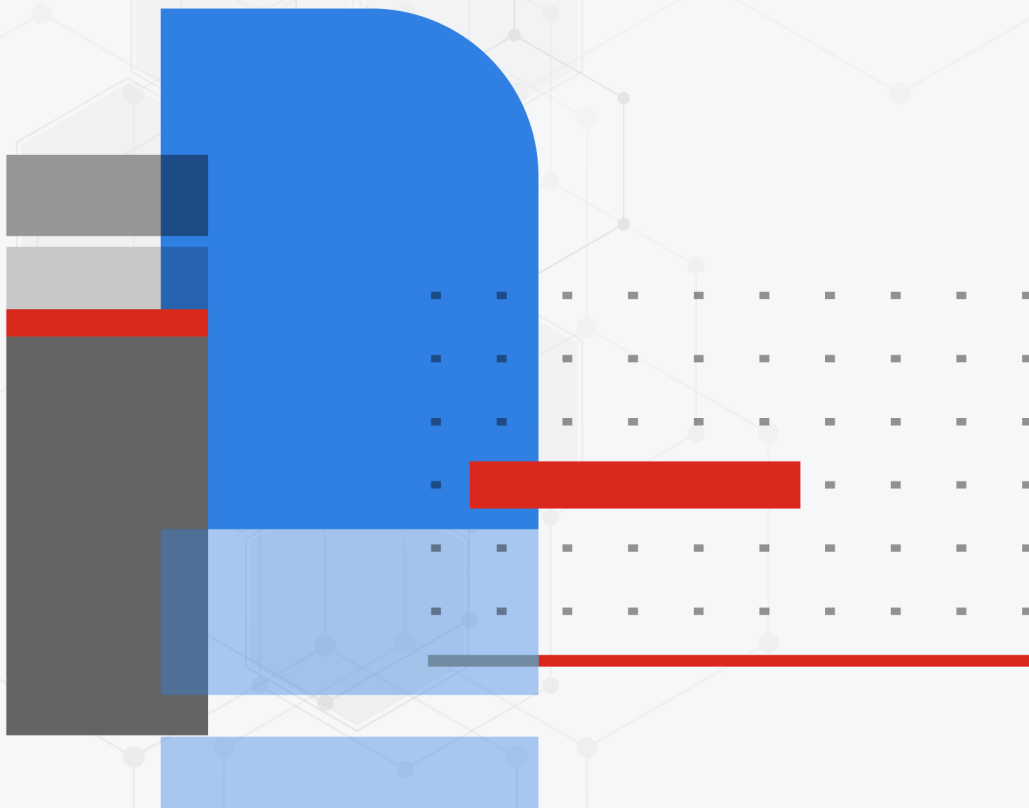
**FORTINET DOCUMENT LIBRARY**

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/training-certification

**FORTINET TRAINING INSTITUTE**

https://training.fortinet.com

**FORTIGUARD CENTER**

https://www.fortiguard.com

**END USER LICENSE AGREEMENT**

https://www.fortinet.com/doc/legal/EULA.pdf

**FEEDBACK**

Email: techdoc@fortinet.com

# TABLE OF CONTENTS

# Change Log

| Date | Change Description |
| --- | --- |
| 05/09/2022 | CMDB Device APIs added. The following API sections were added: Event/Query Worker Configuration API, and Performance and Health API. |
| 06/09/2022 | Lookup Table Integration section updated: POST pub/lookupTable and GET pub/lookup Table. |
| 06/20/2022 | Updated INPUT URL for Update Device by Id, Get Device Custom Property, and Update Device Custom Property. |
| 07/26/2022 | Added FortiGate Watchlist Integration APIs to Watchlist Integration section. |
| 11/29/2022 | Appendix: Current Thresholds for Health Status section updated. |
| 02/24/2023 | Polling API Specifications, Events and Report Integration - Request, Polling, Results API, and Dashboard Integration - Add a Dashboard updated for 6.7.x. |
| 06/01/2023 | Corrected Input URL for Update Device by Id. |
| 06/06/2023 | Added note that 6.7.5 and later API documentation transitioning to https://fndn.fortinet.net/index.php?/fortiapi/2627-fortisiem/. |
| 06/13/2023 | Updated Polling API Specifications Input URL under Events and Report Integration. |
| 08/03/2023 | Updated Results API Specifications Input URL under Events and Report Integration. |

# Overview

> FortiSIEM 6.7.5 and later API documentation is transitioning to https://fndn.fortinet.net/index.php?/fortiapi/2627-fortisiem/. Fortinet recommends checking this link first for the latest API updates.

FortiSIEM provides integrations that allows you to query and make changes to the CMDB, Dashboard, query events, and send incident notifications. Most of these integrations are via REST API.

This document provides integration specifications and example usage.

- CMDB Integration
- Dashboard Integration
- Event/Query Worker Configuration API
- Events and Report Integration
- External Help Desk/CMDB Integration
- External Threat Intelligence Integration
- Incident Integration
- Performance and Health API
- Rest API to Return Worker Queue State
- Watchlist Integration
- Example Usage
- Appendix
  - Description of Device Attributes
  - Description of Health JSON Attributes
  - Current Thresholds for Health Status

# CMDB Integration

The following APIs are available for interacting with the FortiSIEM CMDB.

- Organization API
- Discovery and Monitoring API
- CMDB Device API

**Organization API**

1. Add or Update an Organization
2. Get the List of Monitored Organizations

**Discovery and Monitoring API**

1. Create or Update Device Credentials
2. Discover Devices
3. Get the List of Monitored Devices and Attributes
4. Add, Update or Delete Device Maintenance Schedule
5. Update Device Monitoring

**CMDB Device API**

1. Get Short Description of All Devices
2. Get Short Description of All Devices in an Address Range
3. Get Full Information about One Device
4. Get a Section of Information (Applications, Interfaces, Processors, Storage) about One Device
5. Get Agent Status for a Specific Host
6. Add CMDB Device(s)
7. Delete CMDB Device(s)
8. Get CMDB Device List
9. Get Device Add Request Status
10. Get Device Custom Property
11. Update Device by Id
12. Update Device Custom Property

## Add or Update an Organization

This API enables you to add or update an Organization in Service Provider deployments.

| Release Added | 5.1 |
|---|---|
| Methodology | REST API based: Caller makes an HTTP(S) request with an input XML containing the organization information using organization name as key. |
| Request URL | • **Add an organization:**<br>`https://<FortiSIEM_Supervisor_IP>/phoenix/rest/organization/add`<br>• **Update an organization:**<br>`https://<FortiSIEM_Supervisor_IP>/phoenix/rest/organization/update` |
| Input Parameters | Organization definition file |
| Input Credentials | • **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.<br>Curl example: `curl -k -u super/admin:Admin*123`<br>• **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.<br>Curl example with super organization: `curl -k -u super/admin:Admin*123`<br>If querying for a specific organization, replace "super" with the organization name. |
| Input XML | Contains organization details - the key is the organization name, which means that entries with the same name will be merged. |
| Output | None |

Refer to Example Usage for adding or updating an Organization.

# Get the List of Monitored Organizations

This API enables you to get the list of monitored organizations in Service Provider deployments.

| Release Added | 5.1 |
|---|---|
| Methodology | REST API based: Caller makes an HTTP(S) request with an input XML (optional). An output XML is returned. |
| Input URL | `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/config/Domain` |
| Input Credentials | • **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.<br>Curl example: `curl -k -u super/admin:Admin*123`<br>• **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.<br>Curl example with super organization: `curl -k -u super/admin:Admin*123`<br>If querying for a specific organization, replace "super" with the organization name. |

| Output | An XML that contains Organization id, Organization name, Status, Included and Excluded IP range. |
|---|---|

Refer to Example Usage to get the list of monitored organizations.

# Create or Update Device Credentials

This API enables you to create or update device credentials in Enterprise and Service Provider deployments.

The key is the credential name in the input XML. If a credential with the same name exists, then the credential in the database will be updated with the new content.

| Release Added | 5.1 |
|---|---|
| Methodology | REST API based: Caller makes an HTTP(S) request with an input XML. |
| Request URL | `https://<FortiSIEM_Supervisor_`<br>`IP>/phoenix/rest/deviceMon/updateCredential` |
| Input Credentials | • **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.<br>Curl example: `curl -k -u super/admin:Admin*123`<br>• **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.<br>Curl example with super organization: `curl -k -u super/admin:Admin*123`<br>If querying for a specific organization, replace "super" with the organization name. |
| Input XML | An XML file containing credentials and IP to credential mappings. |
| Output | An HTTP status code. |

Refer to Example Usage creating or updating device credentials.

# Discover Devices

This API enables you to discover devices in Enterprise and Service Provider deployments.

| Release Added | 5.1 |
|---|---|
| Methodology | REST API based: Caller makes an HTTP(S) request with an input XML containing the devices to be discovered. An output XML containing the task Id is returned. The task Id can then be used to get the status of the discovery results. |
| Request URL | • **Send Discovery request:**<br>`https://<FortiSIEM_Supervisor_`<br>`IP>/phoenix/rest/deviceMon/discover` |

| | |
|---|---|
| | • **Get Discovery result:**<br>`https://<FortiSIEM_Supervisor_`<br>`IP>/phoenix/rest/deviceMon/status?taskId=XXX` |
| **Input Credentials** | • **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.<br>Curl example: `curl -k -u super/admin:Admin*123`<br>• **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.<br>Curl example with super organization: `curl -k -u super/admin:Admin*123`<br>If querying for a specific organization, replace "super" with the organization name. |
| **Output** | • Discovery request: XML containing task Id.<br>• Discovery result: XML containing discovered devices and attributes. |

Refer to Example Usage for discovering devices.

# Get the List of Monitored Devices and Attributes

This API enables to get the list of monitored devices and attributes in Enterprise and Service Provider deployments.

| | |
|---|---|
| **Release Added** | 5.1 |
| **Methodology** | REST API based: Caller makes an HTTP(S) request with an input XML (optional). An output XML is returned. |
| **Input URL** | `https://<FortiSIEM_Supervisor_`<br>`IP>/phoenix/rest/deviceInfo/monitoredDevices` |
| **Input Credentials** | • **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.<br>Curl example: `curl -k -u super/admin:Admin*123`<br>• **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.<br>Curl example with super organization: `curl -k -u super/admin:Admin*123`<br>If querying for a specific organization, replace "super" with the organization name. |
| **Output** | An XML that contains device name, device type, organization name and list of monitored attributes. |

Refer to Example Usage to get the list of monitored devices and attributes.

# Add, Update or Delete Device Maintenance Schedule

This API enables you to add, update or delete device maintenance schedule in Enterprise deployments and Service Provider deployments.

| | |
|---|---|
| **Release Added** | 5.1 |
| **Methodology** | REST API based: Caller makes an HTTP(S) request with an input XML (optional). |
| **Input URL** | • **For adding or updating:**<br>`https://<FortiSIEM_Supervisor_IP>/phoenix/rest/deviceMaint/update`<br>• **For deleting:**<br>`https://<FortiSIEM_Supervisor_IP>/phoenix/rest/deviceMaint/delete` |
| **Input Parameters** | An XML file Containing devices and maintenance calendar updates. |
| **Input Credentials** | • **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.<br>Curl example: `curl -k -u super/admin:Admin*123`<br>• **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.<br>Curl example with super organization: `curl -k -u super/admin:Admin*123`<br>If querying for a specific organization, replace "super" with the organization name. |
| **Output** | An HTTP status code. |

Refer to *Example Usage* for adding or updating device maintenance schedule and for deleting device maintenance schedule.

# Update Device Monitoring

This API enables you to update device monitoring in Enterprise and Service Provider deployments.

| | |
|---|---|
| **Release Added** | 5.1 |
| **Methodology** | REST API based: Caller makes an HTTP(S) request with an input XML (optional). |
| **Input URL** | `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/deviceMon/updateMonitor` |
| **Input Credentials** | • **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.<br>Curl example: `curl -k -u super/admin:Admin*123`<br>• **Service Provider deployments:** User name and password of Super Global account or |

| | |
|---|---|
| | Organization specific account and name. Make sure that the account has the appropriate access.<br>Curl example with super organization: `curl -k -u super/admin:Admin*123`<br>If querying for a specific organization, replace "super" with the organization name. |
| **Input Parameters** | Input XML containing the updates to device monitoring configuration. |
| **Output** | HTTP Status Code |

Refer to Example Usage for updating device monitoring.

# Get Short Description of All Devices

| | |
|---|---|
| **Release Added** | 5.1 |
| **Methodology** | REST API based: Caller makes an HTTP(S) request with an input XML. An output XML is returned. |
| **Input URL** | • **Enterprise deployments:**<br>`https://<FortiSIEM_Supervisor_`<br>`IP>/phoenix/rest/cmdbDeviceInfo/devices`<br>• **Service Provider deployments:**<br>`https://<FortiSIEM_Supervisor_`<br>`IP>/phoenix/rest/cmdbDeviceInfo/devices&organization=ACME` |
| **Input Credentials** | • **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.<br>Curl example: `curl -k -u super/admin:Admin*123`<br>• **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.<br>Curl example with super organization: `curl -k -u super/admin:Admin*123`<br>If querying for a specific organization, replace "super" with the organization name. |
| **Output** | An XML that contains a short set of attributes for each device, including:<br>• Host Name<br>• Access IP<br>• Creation Method<br>• Description<br>• Vendor, Model, version<br>• Contact info<br>• Location<br>• Uptime<br>• Hardware Model<br>• Serial Number |

> • Business Service Groups to which the device belongs

# Get Short Description of All Devices in an Address Range

| Release Added | 5.1 |
|---|---|
| Methodology | REST API based: Caller makes an HTTP(S) request with an input XML. An output XML is returned. |
| Input URL | • **Enterprise deployments:**<br>`https://<FortiSIEM_Supervisor_IP>/phoenix/rest/cmdbDeviceInfo/devices?includeIps=<includeIpSet>&excludeIps=<excludeIpSet>`<br>• **Service Provider deployments:**<br>`https://<FortiSIEM_Supervisor_IP>/phoenix/rest/cmdbDeviceInfo/devices?includeIps=<includeIpSet>&excludeIps=<excludeIpSet>&organization=ACME` |
| Input Credentials | • **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.<br>Curl example: `curl -k -u super/admin:Admin*123`<br>• **Service Provider deployments:** User name and password of any FortiSIEM account for the ACME organization. Make sure that the account has the appropriate access. Curl example with ACME organization: `curl -k -u ACME/admin:Admin*123` |
| Output | An XML that contains short description of devices with access IPs in the specified address range. |

## Formatting for the <IncludeIPset> and <ExcludeIPset> Attributes

Both `<includeIpSet>` and `<excludeIpSet>` can take any of these forms:

- IPaddress
- IPaddress1,IPaddress2
- IPaddress1-IPaddress2
- IPaddress1,IPaddress2-IPaddress3,IPaddress4,IPaddress5-IPaddress6

### Examples

- If you want all devices in the range `192.168.20.1-192.168.20.100`, then issue the API:<br>`https://<FortiSIEM_Supervisor_IP>/phoenix/rest/cmdbDeviceInfo/devices?includeIps=192.168.20.1-192.168.20.100`
- If you want all devices in the range `192.168.20.1-192.168.20.100`, but want to exclude `192.168.20.20, 192.168.20.25,` then issue the API:<br>`https://<FortiSIEM_Supervisor_`

```
IP>/phoenix/rest/cmdbDeviceInfo/devices?includeIps=192.168.20.1-
192.168.20.100&excludeIps=192.168.20.20,192.168.20.25
```

- If you want all devices in the range 1`92.168.20.1-192.168.20.100`, but want to exclude `192.168.20.20-192.168.20.25`, then issue the API:
  ```
  https://<FortiSIEM_Supervisor_
  IP>/phoenix/rest/cmdbDeviceInfo/devices?includeIps=192.168.20.1-
  192.168.20.100&excludeIps=192.168.20.20-192.168.20.25
  ```

# Get Full Information about One Device

| Release Added | 5.1 |
|---|---|
| Methodology | REST API based: Caller makes an HTTP(S) request with an input XML (optional). An output XML is returned. |
| Input URL | • **Enterprise deployments:**<br>`https://<FortiSIEM_Supervisor_`<br>`IP>/phoenix/rest/cmdbDeviceInfo/device?ip=`<br>`<deviceIp>&loadDepend=true`<br>• **Service Provider deployments:**<br>`https://<FortiSIEM_Supervisor_IP>/phoenix/rest/cmdbDeviceInfo/`<br>`device?ip=<deviceIp>&loadDepend=true&organization=ACME` |
| Input Credentials | • **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.<br>Curl example: `curl -k -u super/admin:Admin*123`<br>• **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.<br>Curl example with super organization: `curl -k -u super/admin:Admin*123`<br>If querying for a specific organization, replace "super" with the organization name. |
| Output | An XML that contains full information FortiSIEM has discovered about a device. |

# Get a Section of Information (Applications, Interfaces, Processors, Storage) about One Device

| Release Added | 5.1 |
|---|---|
| Methodology | REST API based: Caller makes an HTTP(S) request with an input XML (optional). An output XML is returned. |
| Input URL | • **Enterprise deployments:**<br>`https://<FortiSIEM_Supervisor_`<br>`IP` |

```
>/phoenix/rest/cmdbDeviceInfo/device?ip=<
deviceIp>&loadDepend=true&fields=<sectionName>
```

- **Service Provider deployments:**
  ```
  https://<FortiSIEM_Supervisor_
  IP
  >/phoenix/rest/cmdbDeviceInfo/device?ip=<
  deviceIp>&loadDepend=true&fields= <sectionName>&organization=ACME
  ```

| | |
|---|---|
| **Input Credentials** | • **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.<br>Curl example: `curl -k -u super/admin:Admin*123`<br>• **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.<br>Curl example with super organization: `curl -k -u super/admin:Admin*123`<br>If querying for a specific organization, replace "super" with the organization name. |
| **Output** | An XML that contains the specified section discovered for the device. |

**Options for `<sectionName>`:** `applications`, `interfaces`, `processors` or `storages`

Refer to Example Usage to get CMDB device info.

# Get Agent Status for a Specific Host

This API enables you to get Linux and Windows Agent status.

| | |
|---|---|
| **Release Added** | 5.2.5 |
| **Methodology** | REST API based: Caller makes an HTTPS request with query parameters: `orgId`, `hostName`. |
| **Request URL** | `https://<FortiSIEM_Supervisor_`<br>`IP>/phoenix/rest/agentStatus/all?request=<orgId>,<hostName>` |
| **Input Credentials** | • **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.<br>Curl example: `curl -k -u super/admin:Admin*123`<br>• **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.<br>Curl example with super organization: `curl -k -u super/admin:Admin*123`<br>If querying for a specific organization, replace "super" with the organization name. |
| **Input Parameters** | Query parameters: `orgId`, `hostName`. |
| **Output** | An XML file containing Type, AgentStatus, PolicyID, HeartbeatTime, LastEventReceiveTime |

Refer to Example Usage to get the list of monitored devices and attributes.

# Add CMDB Device(s)

This API provides the ability to add one or more devices to CMDB. This is an asynchronous request that should be used as follows:

- Submit the device add request. A task id will be returned
- Get the device addition status by querying with this task id (See Get Device Add Request Status API)

| | |
|---|---|
| **Release Added** | 6.5.0 |
| **Input URL** | `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/device/discovery/add` |
| **Input Credentials** | • **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.<br>Curl example: `curl -k -u super/admin:Admin*123`<br><br>• **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.<br>Curl example with super organization: `curl -k -u super/admin:Admin*123`<br>If querying for a specific organization, replace "super" with the organization name. |
| **HTTP Method** | POST |
| **Request Body** | You need to create an XML for the device attributes and pass it in the HTTP request. A sample XML file is File5_AddDeviceExample.xml and the schema file XSD is File6_device.xsd. For an explanation the attribute definitions, see Appendix - Description of Device Attributes. |
| **Output** | When the request succeeds (HTTP response code 200), a taskId will be returned. You can query Device add status using this task Id in a separate API (see Get Device Add Request Status).<br><br>`<response>`<br>`    <status>Discovery xml is queued</status>`<br>`    <sourceIdentifier>RESTAPI_<TaskId></sourceIdentifier>`<br>`</response>` |

# Delete CMDB Device(s)

This POST API enables you to delete one or more CMDB devices by specifying device IDs. The list of device ids can be obtained via the Get CMDB Device List API.

| | |
|---|---|
| **Release Added** | 6.5.0 |
| **Input URL** | https://*<FortiSIEM_Supervisor_IP>*/phoenix/rest/device/list/delete |
| **Input Credentials** | • **Enterprise deployments:** User name and password of any FortiSIEM account |

| | that has the appropriate access. Use "super" as the organization for Enterprise deployments.<br>Curl example: `curl -k -u super/admin:Admin*123`<br>• **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.<br>Curl example with super organization: `curl -k -u super/admin:Admin*123`<br>If querying for a specific organization, replace "super" with the organization name. |
|---|---|
| **HTTP Method** | POST |
| **Request Body** | The request body should be a JSON with a list of device ids. Note that the list of device ids can be obtained via the Get CMDB Device List API.<br>Input JSON array format: [id1, id2]<br>Request Body example:<br>[id1, id2] |
| **Output** | When the request succeeds (HTTP response code 200), a JSON object is returned. It contains the list of device ids that were successfully deleted and the list of device ids for which delete failed.<br>Sample JSON follows.<br><br>`{`<br>`  "success": "[968352]",`<br>`  "failed": "[968351,968353]"` |

# Get CMDB Device List

You can use this GET API to retrieve list of devices with specific organization ID and device IP/host name.

| **Release Added** | 6.5.0 |
|---|---|
| **Input URL** | `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/device/list?orgId=<org_id>&accessIp=<access_ip>&name=<name>` |
| **Input Credentials** | • **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.<br>Curl example: `curl -k -u super/admin:Admin*123`<br>• **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.<br>Curl example with super organization: `curl -k -u super/admin:Admin*123`<br>If querying for a specific organization, replace "super" with the organization name. |
| **HTTP Method** | GET |

| Request Path Parameters | Field | Type | Description |
|---|---|---|---|
| | org_id | long | Organization ID which device belongs to. This is a required field. |
| | access_ip | string | Device IP Address. Must be an exact match. Either access_ip or name is required. |
| | name | string | Host name of the device. Partial match is allowed. Either access_ip or name is required. |

| Output | When the request succeeds (HTTP response code 200), a JSON object is returned. It contains key attributes of the CMDB devices matching the request filter. |
|---|---|
| | Sample JSON follows. |
| | <pre>{<br>  "id": 968352,<br>  "orgId": 1,<br>  "orgName": "Super",<br>  "hostName": "FSM_Test_6501741_5835",<br>  "accessIp": "172.30.58.35",<br>  "deviceType": "Redhat Linux"<br>}<br>]</pre> |
| | If there are no matching devices, then the JSON is empty. |

| Output Key Fields | Field | Type | Description |
|---|---|---|---|
| | id | long | Device ID in FortiSIEM CMDB |
| | orgId | long | Organization ID which device belongs to. |
| | orgName | string | Organization Name |
| | hostName | string | Host Name |
| | accessIp | string | Device IP Address |
| | deviceType | string | Device Type |

# Get Device Add Request Status

You can use this API to get the status of device add request with specific task id.

| Release Added | 6.5.0 |
|---|---|
| Input URL | https://*<FortiSIEM_Supervisor_IP>*/phoenix/rest/device/list/source?identifier=RESTAPI_*<TaskId>* |
| Input Credentials | • **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.<br>Curl example: `curl -k -u super/admin:Admin*123`<br>• **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access. |

| | |
|---|---|
| | Curl example with super organization: `curl -k -u super/admin:Admin*123` If querying for a specific organization, replace "super" with the organization name. |
| **HTTP Method** | GET |
| **Request Path Parameter** | Replace <*TaskId*> with long value in the URL. The TaskId is obtained from the response in the Add CMDB Device(s) API. |
| **Output** | When the request succeeds (HTTP response code 200), a JSON object is returned. It contains key attributes of the devices that were added to CMDB as part of the request with the specified TaskId. Sample JSON follows. <br><br>```[<br>  {<br>    "id": 968352,<br>    "orgId": 1,<br>    "orgName": "Super",<br>    "hostName": "FSM_Test_6501741_5835",<br>    "accessIp": "172.30.58.35",<br>    "deviceType": "Redhat Linux"<br>  }<br>]```<br><br>When the request fails, response contains failed reason. **Note**: Failed devices are not provided in this release. |
| **Output Key Fields** | **Field** **Type** **Description**<br>id long Device ID in FortiSIEM CMDB<br>orgId long Organization ID which device belongs to<br>orgName string Organization Name<br>hostName string Host Name<br>accessIp string Device IP Address<br>deviceType string Device Type |

# Get Device Custom Property

This GET API returns the device properties for a particular device specified by organization name, organization ID, access IP or host name. Only the properties that are set are returned.

| | |
|---|---|
| **Release Added** | 6.5.0 |
| **Input URL** | https://<*FortiSIEM_Supervisor_IP*>/phoenix/rest/cmdbDeviceInfo/properties?organization=<*org_name*>&orgId=<*org_id*>&ip=<*device_ip*>&name=<*hostname*> |
| **Input Credentials** | • **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments. |

| | Curl example: `curl -k -u super/admin:Admin*123` |
| --- | --- |
| | • **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access. Curl example with super organization: `curl -k -u super/admin:Admin*123` If querying for a specific organization, replace "super" with the organization name. |
| **HTTP Method** | GET |
| **Request Path Parameters** | <table><tr><td>**Field**</td><td>**Type**</td><td>**Description**</td></tr><tr><td>org_name</td><td>string</td><td>Organization name</td></tr><tr><td>org_id</td><td>long</td><td>Organization ID. Required field.</td></tr><tr><td>ip</td><td>string</td><td>Device Access IP. Must be an exact match. Either ip or name is required.</td></tr><tr><td>name</td><td>string</td><td>Host name of the device. Either ip or name is required.</td></tr></table> |
| **Output** | When the request succeeds (HTTP response code 200), then an XML is returned with the set properties for that device. Schema XSD file is File9_device_properties.xsd. |

# Update Device by Id

This POST API allows user to update the CMDB device attributes for a CMDB Device. The device need to specified device id, that can be obtained via the Get CMDB Device List API. Only the attributes that need to be updated should be sent as part of API.

| | |
| --- | --- |
| **Release Added** | 6.5.0 |
| **Input URL** | `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/device/update?deviceId=<device_id>&updateMode=OVERWRITE|APPEND` |
| **Input Credentials** | • **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments. Curl example: `curl -k -u super/admin:Admin*123` • **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access. Curl example with super organization: `curl -k -u super/admin:Admin*123` If querying for a specific organization, replace "super" with the organization name. |
| **HTTP Method** | POST |
| **Request Path Parameters** | <table><tr><td>**Field**</td><td>**Type**</td><td>**Description**</td></tr><tr><td>deviceId</td><td>string</td><td>Device Id in CMDB - ids can be obtained via the Get CMDB Device List API.</td></tr><tr><td>updateMode</td><td>long</td><td>Two values are allowed.<br>• OVERWRITE – meaning overwrite the value like name or</td></tr></table> |

| Field | Type | Description |
|---|---|---|
| | | • APPEND – meaning add like network interface |
| Request Body | | You need to create an XML as in Add CMDB Device(s) API to include the device attributes that you want to update and pass it in the HTTP request.<br><br>A sample XML file for OVERWRITE-ing a device host name is File7_OVERWRITE_ DeviceExample.xml. A sample XML file for APPEND-ing a device network Interface is File7_APPEND_DeviceExample.xml. The schema XSD is File8_ deviceAPPENDExample.xsd. For an explanation the attribute definitions, see Appendix - Description of Device Attributes. |
| Output | | When the request succeeds (HTTP response code 200), the following message will appear depending on the update status.<br>• If update succeeds, a message "Successfully updated device" is returned.<br>• If update fails, a proper error message e.g. "Invalid Device Id" is returned.<br>Invalid attributes are ignored, and valid attributes are updated. |

# Update Device Custom Property

This PUT API provides a way to modify the device properties of one or more devices.

| | |
|---|---|
| **Release Added** | 6.5.0 |
| **Input URL** | https://*<FortiSIEM_Supervisor_IP>*/phoenix/rest/cmdbDeviceInfo/properties |
| **Input Credentials** | • **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.<br>Curl example: `curl -k -u super/admin:Admin*123`<br>• **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.<br>Curl example with super organization: `curl -k -u super/admin:Admin*123`<br>If querying for a specific organization, replace "super" with the organization name. |
| **HTTP Method** | PUT |
| **Request Body** | The modified properties and the list of devices need to be specified in an XML file in the body. The XSD is File9_device_properties.xsd. Key fields are<br>• ipAddr: the comma separated list of device access IP addresses for which properties have to be set<br>• propertyName: the name of the property<br>• propertyValue: the new value |

| Field | Type | Description |
|---|---|---|
| Body | Properties XML | XML format can be obtained from - `/rest/pub/cmdbDeviceInfo /properties` |

A sample XML example is Sample_Device_Custom_Property_Request_Body.xml.

| Output | When the request succeeds (HTTP response code 200), the properties are modified as defined in the request. |

# Dashboard Integration

This API enables you to interact with FortiSIEM Dashboard. You can perform the following operation:

- Add a Dashboard Folder

## Add a Dashboard Folder

This API enables you to add Dashboard folders to an Organization.

| | |
|---|---|
| **Release Added** | 5.1 |
| **Methodology** | REST API based: Caller makes an HTTP(S) request with an input XML. |
| **Request URL** | **Add a Dashboard folder to an Organization:**<br>`https://<FortiSIEM_Supervisor_IP>/phoenix/rest/dashboard/html/add` |
| **Input Parameters** | Dashboard folder definition file. |
| **Input Credentials** | **Enterprise deployments**: User name and password of any FortiSIEM account. Use "super" as the organization for Enterprise deployments.<br>Curl example: `curl -k -u super/admin:Admin*123`<br><br>**Service Provider deployments**: User name and password of Super or organization specific account.<br>Curl example with super organization: `curl -k -u super/admin:Admin*123`<br>**Note**: If querying for a specific organization, replace "super" with the organization name. |
| **Input XML** | Contains dashboard details to be included in this folder:<br>- Dashboard folder name<br>- Organization name<br>- Time range<br>- Dashboard type |
| **Output** | An HTTP status code. |

Refer to Example Usage for adding a Dashboard folder.

# Events and Report Integration

This REST API based caller makes an HTTP(S) request with an input XML that defines the query. Since a query can take some time and the number of returned results can be large, the query works as follows:

1. Caller submits the query and gets a Query Id back from FortiSIEM. This is done via Request API.
2. Caller polls for query progress and waits until the query is completed. This is done via Polling API.
3. When the query is completed, Caller gets the results via Results API.
   a. Caller gets the total number of query results and the query result fields.
   b. Caller gets the results - one chunk at a time.

This API provides a way to programmatically run any query on the event data. Following are the specifications for:

- Request API
- Polling API
- Results API

# Request API Specifications

| | |
|---|---|
| **Release Added** | 5.1 |
| **Input URL** | `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/query/eventQuery` |
| **Input Parameters** | XML file containing the query parameters. |
| **Input Credentials** | • **Enterprise deployments**: User name and password of any FortiSIEM account. Use "super" as the organization for Enterprise deployments.<br>Curl example: `curl -k -u super/admin:Admin*123`<br>• **Service Provider deployments**: User name and password of Super account for getting incidents for all organizations. If incidents for a specific organization are needed, then an organization-specific account and an organization name is needed.<br>Curl example with super organization: `curl -k -u super/admin:Admin*123`<br>**Note**: If querying for a specific organization, replace "super" with the organization name. |
| **Output** | `queryId` or an error code if there is a problem in handling the query or the query format. |

# Polling API Specifications

The request will poll until the server completes the query.

| | |
|---|---|
| **Release Updated** | 6.7.0 |
| **Input URL** | https://*<FortiSIEM_Supervisor_IP>*/phoenix/rest/query/progress/*<requestId>*, *<expireTime>* |
| **Output** | progress (pct)<br>Until progress reaches 100 (completed), caller needs to continue polling FortiSIEM. This is because the server may need to aggregate the results or insert meta-information before sending the results. |

# Results API Specifications

| | |
|---|---|
| **Release Added** | 5.1 |
| **Input URL** | `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/query/events/<requestId>,<expireTime>/<begin>/<end>` |
| **Output** | totalCount (first time) and an XML containing the incident attributes.<br>For the first call, **begin** = 0 and **end** can be 1000. You must continuously query the server by using the same URL, but increasing the `begin` and `end` until the totalCount is reached. |

Refer to Example Usage for a sample query.

# Event/Query Worker Configuration API

These APIs enables you to query and make changes to event worker or query worker configurations.

- Get Event Worker
- Add Event Worker
- Delete Event Worker
- Get Query Worker
- Add Query Worker
- Delete Query Worker

## Get Event Worker

This GET API retrieves the list of Event Workers defined in FortiSIEM.

**Release Added**: 6.5.0

**Input URL**   `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/system/eventworker`

### Input Credentials

- **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.
  Curl example: `curl -k -u super/admin:Admin*123`
- **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.
  Curl example with super organization: `curl -k -u super/admin:Admin*123`
  If querying for a specific organization, replace "super" with the organization name.

## HTTP Method

GET

## Output

When the request succeeds (HTTP response code 200), then a JSON file is returned with the list of Event Workers as defined in GUI. Sample JSON follows.

```
{
  "addresses": [
    "wk1.acme.com",
    "192.0.2.0"
```

```
    ]
}
```

# Add Event Worker

This POST API enables you to add an Event Worker to the list of Event Workers defined in FortiSIEM.

**Release Added**: 6.5.0

**Input URL**  `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/system/add/eventworker`

## Input Credentials

- **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.
  Curl example: `curl -k -u super/admin:Admin*123`
- **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.
  Curl example with super organization: `curl -k -u super/admin:Admin*123`
  If querying for a specific organization, replace "super" with the organization name.

## HTTP Method

POST

## Request Body

| Field | Type | Description |
|-------|------|-------------|
| Body | JSON array of Event Worker addresses entry | Event Worker FQDN or IP |

## Request Body Example

```
{
"addresses": ["wk1.acme.com","wk2.acme.com"]
}
```

## Output

When the request succeeds (HTTP response code 200), then a JSON file is returned with the list of successful and failed additions.

```
{
  "success": [
```

```
      "Event worker added: wk1.acme.com"
  ],
  "failed": [
    "Not a valid worker address: invalidworkaddress"
  ]
}
```

# Delete Event Worker

This POST API enables you to delete an Event Worker from the list of Event Workers defined in FortiSIEM.

**Release Added**: 6.5.0

**Request URL** `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/system/delete/eventworker`

## Input Credentials

- **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.
  Curl example: `curl -k -u super/admin:Admin*123`
- **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.
  Curl example with super organization: `curl -k -u super/admin:Admin*123`
  If querying for a specific organization, replace "super" with the organization name.

## HTTP Method

POST

## Request Body

| Field | Type | Description |
|-------|------|-------------|
| Body | JSON array of Event Worker addresses entry | Event Worker FQDN or IP |

## Request Body Example

```
{
"addresses": ["wk1.acme.com","wk2.acme.com"]
}
```

## Output

When the request succeeds (HTTP response code 200), then a JSON file is returned with the list of successful and failed additions.

```
{
  "success": [
    "Event worker deleted: wk1.acme.com"
  ],
  "failed": [
    "Not a valid worker address: invalidworkaddress"
  ]
}
```

# Get Query Worker

This GET API retrieves the list of Query Workers defined in FortiSIEM.

**Release Added**: 6.5.0

 **Input URL**   `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/system/queryworker`

## Input Credentials

- **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.
  Curl example: `curl -k -u super/admin:Admin*123`
- **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.
  Curl example with super organization: `curl -k -u super/admin:Admin*123`
  If querying for a specific organization, replace "super" with the organization name.

## HTTP Method

GET

## Output

When the request succeeds (HTTP response code 200), then a JSON file is returned with the list of Query Workers as defined in GUI. Sample JSON follows.

```
{
  "addresses": [
    "wk1.acme.com",
    "192.0.2.84"
  ]
}
```

# Add Query Worker

This POST API is available to add Query Worker IP addresses or resolvable host names.

**Release Added**: 6.5.0

**Input URL**  `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/system/add/queryworker`

## Input Credentials

- **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.
  Curl example: `curl -k -u super/admin:Admin*123`
- **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.
  Curl example with super organization: `curl -k -u super/admin:Admin*123`
  If querying for a specific organization, replace "super" with the organization name.

## HTTP Method

POST

## Request Body

| Field | Type | Description |
|-------|------|-------------|
| Body | JSON array of Query Worker addresses entry | Query Worker FQDN or IP |

## Request Body Example

```
{
"addresses": ["wk1.acme.com",”wk2.acme.com”]
}
```

## Output

When the request succeeds (HTTP response code 200), then a JSON file is returned with the list of successful and failed additions.

```
{
  "success": [
    "Query worker added: wk1.acme.com"
  ],
  "failed": [
    "Not a valid worker address: invalidworkaddress"
```

```
    ]
}
```

# Delete Query Worker

This POST API enables you to delete a Query Worker from the list of Query Workers defined in FortiSIEM.

**Release Added**: 6.5.0

 **Request URL** `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/system/delete/queryworker`

## Input Credentials

- **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.
  Curl example: `curl -k -u super/admin:Admin*123`
- **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.
  Curl example with super organization: `curl -k -u super/admin:Admin*123`
  If querying for a specific organization, replace "super" with the organization name.

### HTTP Method

POST

## Request Body

| Field | Type | Description |
|-------|------|-------------|
| Body | JSON array of Query Worker FQDN or IP | Query Worker FQDN or IP |

## Request Body Example

```
{
"addresses": ["wk1.acme.com","wk2.acme.com"]
}
```

## Output

When the request succeeds (HTTP response code 200), then a JSON file is returned with the list of successful and failed additions.

```
{
  "success": [
```

```
      "Query worker deleted: wk1.acme.com"
    ],
    "failed": [
      "Not a valid worker address: invalidworkaddress"
    ]
}
```

# External Help Desk/CMDB Inbound Integration

FortiSIEM has inbuilt support for ServiceNow and ConnectWise for CMDB and two-way incident integration. Other systems can be supported by creating a new Java plug-in. Follow the instructions in the FortiSIEM Service API which can be obtained from this website: https://filestore.fortinet.com/docs.fortinet.com/upload/FortiSIEMServiceAPIDocs.zip.

# External Threat Intelligence Integration

New external threat intelligence sources can be supported by creating a new Java plug-in. Follow the instructions in the FortiSIEM Service API which can be obtained from this website:
https://filestore.fortinet.com/docs.fortinet.com/upload/FortiSIEMServiceAPIDocs.zip.

# Incident Integration

The follow Incident Integration APIs are available.

- Incident Notification Integration
- Update Incident Attributes API
- JSON API Incident Integration

# Incident Notification Integration

FortiSIEM can send notifications via email/SMS, HTTPS, SNMP traps, and over the FortiSIEM API.

These topics describe the notification types:

- Email/SMS
- HTTPS
- SNMP Trap
- API
- Get Triggering Event IDs for One or More Incidents

## Notification via Email

Email is the most common form of incident notification. While FortiSIEM has a default email format, users can also create their own email templates from the FortiSIEM GUI.

The screenshots show three types of email that can be sent depending on whether an incident is NEW, UPDATEd or CLEARed.

**Release Added**: 5.1

### NEW



[New] qa-v-win03-ads: Server CPU Warning

notify@accelops.net

To: Partha Bhattacharya <partha@accelops.net>

[New] qa-v-win03-ads: Server CPU Warning

Incident ID: 333516
Time: Wed Aug 11 09:53:00 PDT 2010
Severity: MEDIUM (5)
Incident Count: 1

Rule
  Rule Name: Server CPU Warning
  Rule Description: Detects that server CPU has reached a warning level (between 75% and 85% based on 2 successive readings in a 10 minute interval

Target
  Host IP: 172.16.10.15
  Host Name: qa-v-win03-ads.prospect-hills.net

Detail
  CPU Util: 75.25

Affected Business Services: Auth Service,DHCP/DNS Service

Triggering Attribute(s):
  CPU Util: 75.25

## UPDATE

[Update] ACCELOPS-A804CE: Server Memory Warning

notify@accelops.net

**To:** Partha Bhattacharya <partha@accelops.net>

[Update] ACCELOPS-A804CE: Server Memory Warning

Incident ID: 362034
First Seen Time: Wed Aug 11 13:11:00 PDT 2010
Last Seen Time: Wed Aug 11 16:45:00 PDT 2010
Severity: MEDIUM (5)
Incident Count: 34

Rule
  Rule Name: Server Memory Warning
  Rule Description: Detects that server Memory has reached a warning level (between 75% and 85% based on 2 successive readings in
a 10 minute interval

Target
  Host IP: 172.16.10.139
  Host Name: ACCELOPS-A804CE

Detail
  Memory Util: 78.55

Triggering Attribute(s):
  Memory Util: 78.55

## CLEAR

[Clear] qa-v-win03-ads: Server CPU Critical

notify@accelops.net

**To:** Partha Bhattacharya <partha@accelops.net>

[Clear] qa-v-win03-ads: Server CPU Critical

Incident ID: 382113
Time: Wed Aug 11 16:14:10 PDT 2010
First Seen Time: Wed Aug 11 15:48:00 PDT 2010
Last Seen Time: Wed Aug 11 15:54:00 PDT 2010
Severity: HIGH (9)
Incident Count: 2

Rule
  Rule Name: Server CPU Critical
  Rule Description: Detects that server CPU has reached a critical level (greater than 85% based on 2 successive readings in a 10
minute interval

Target
  Host IP: 172.16.10.15
  Host Name: qa-v-win03-ads.prospect-hills.net

Detail
  CPU Util: 89.00

Affected Business Services: Auth Service,DHCP/DNS Service

Identity And Location
  IP Details
    IP Address: 172.16.10.15
    Domain: PROSPECT-HILLS
    Host Name: QA-V-WIN03-ADS
    First Seen Time: Wed Aug 11 14:58:35 PDT 2010
    Last Seen Time: Wed Aug 11 16:12:13 PDT 2010

## Subject Line Format

```
[New|Update|Clear] <HostName>: <Rule Name>
```

**Body format**

| Section | Field | Description |
|---------|-------|-------------|
| **Affected Business Services** (optional) | | |
| **Generic** | | |
| **Identity and Location** | | - Contains additional information for IP addresses in incident source or target. This information is present only if such information is discovered by FortiSIEM and shown in the Identity and Location tab.<br>- Host name<br>- User<br>- Domain<br>- Nearest switch name/port or VPN gateway or Wireless Controller<br>- First and last seen times for this IP address to identity/location binding |
| **Incident Details** | | Rule-specific details that caused the incident to trigger |
| **Incident Source** | | For security-related incidents, where the incident originated |
| **Incident Target** | | Where the incident occurred, or the target of an IPS alert |
| **Rule** | Rule Name | Name of the rule, repeated in the subject line |
| | Incident Id | Unique ID of the incident in FortiSIEM. An incident can be searched in FortiSIEMby this ID. |
| | Time | Time when this incident occurred |
| | Severity | Incident severity: HIGH|MEDIUM|LOW and a numeric severity in the range 0-10 (0-4 LOW, 5-8 MEDIUM and 9-10 HIGH |
| | Incident Count | How many times this incident has occurred. For NEW incidents, the count is 1. |
| | Rule Description | |
| | Host Name (optional) | |
| | Host IP (optional) | |
| | Other attributes as defined in rule | |
| | Host Name (optional) | |
| | Host IP (optional) | |

# Notification via SMS

SMS notification is a shortened version of email notification.

**Release Added**: 5.1
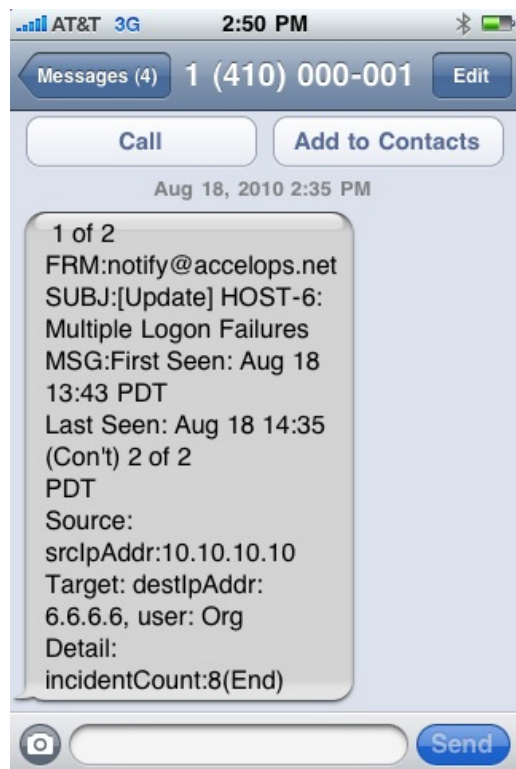


# Notifications via HTTPS

When an incident triggers, FortiSIEM can push an XML file containing Incident details via HTTP(S) POST.

**Release Added**: 5.1

The FortiSIEM `AONotification.xsd` file shows the XML schema for incident notifications.

```
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:element name="incident">
<xs:complexType>
<xs:sequence>
<xs:element type="xs:string" name="name"/>
<xs:element type="xs:string" name="description"/>
<xs:element type="xs:string" name="displayTime"/>
<xs:element type="xs:string" name="incidentSource"/>
<xs:element name="incidentTarget">
<xs:complexType>
        <xs:sequence>
        <xs:element name="entry">
```

```
            <xs:complexType>
                    <xs:simpleContent>
                            <xs:extension base="xs:string">
                                    <xs:attribute type="xs:string" name="attribute"/>
                                    <xs:attribute type="xs:string" name="name"/>
                             </xs:extension>
                    </xs:simpleContent>
            </xs:complexType>
</xs:element>
        </xs:sequence>
        </xs:complexType>
        </xs:element>
<xs:element name="incidentDetails">
        <xs:complexType>
        <xs:sequence>
        <xs:element name="entry">
                <xs:complexType>
                        <xs:simpleContent>
                                <xs:extension base="xs:float">
                                        <xs:attribute type="xs:string" name="name"/>
                                </xs:extension>
                        </xs:simpleContent>
                </xs:complexType>
        </xs:element>
        </xs:sequence>
        </xs:complexType>
</xs:element>
        <xs:element type="xs:string" name="affectedBizSrvc"/>
        <xs:element type="xs:string" name="identityLocation"/>
        </xs:sequence>
        <xs:attribute type="xs:short" name="incidentId"/>
        <xs:attribute type="xs:string" name="ruleType"/>
                <xs:attribute type="xs:byte" name="severity"/>
                <xs:attribute type="xs:byte" name="repeatCount"/>
                <xs:attribute type="xs:string" name="organization"/>
                <xs:attribute type="xs:string" name="status"/>
                </xs:complexType>
        </xs:element>
</xs:schema>
```

The description of each field is as follows:

| Section | Field | Description |
|---------|-------|-------------|
| **Generic** | | |
| | incidentId | Unique ID of the incident in FortiSIEM. An incident can be searched in FortiSIEM by this ID. |
| | ruleId | Unique id of the rule in FortiSIEM |
| | vendor | FortiSIEM |
| | severity | Incident severity: HIGH | MEDIUM | LOW |

| Section | Field | Description |
| --- | --- | --- |
| | organization | The name of the organization for which this incident occurred |
| | status | New, Update or Clear |
| | repeatCout | how many times this incident has occurred |
| | name | Name of the rule that triggered the incident |
| | description | Description of the rule including conditions under which the rule is written to trigger |
| | displayTime | Time when this incident occurred |
| incidentTarget | | Where the incident occurred, or the target of an IPS alert. It consists of attribute, name and value pairs. |
| | attribute | Parsed event attribute id |
| | name | Display name of the attribute. Common examples of attributes are srcIpAddr, destIpAddr, hostIpAddr etc. |
| | value | The attribute's value |
| incidentSource | | For security-related incidents, where the incident originated |
| | attribute | Parsed event attribute id |
| | name | Display name of the attribute. Common examples of attributes are srcIpAddr, destIpAddr, hostIpAddr etc. |
| | value | The attribute's value |
| incidentDetails | | Rule-specific details that caused the incident to trigger shown as an attribute with name and value pairs. |
| | attribute | Parsed event attribute id |
| | name | Display name of the attribute Common examples of attributes are srcIpAddr, destIpAddr, hostIpAddr etc. |
| | value | The attribute's value |
| affectedBizSrvc | | A comma-separated list of business service names |
| deviceDetails | | Contains additional information for IP addresses in incident source or target. This information is present only if such information is discovered by FortiSIEM and shown in the Identity and Location tab.<br>• ipAddr |

| Section | Field | Description |
|---------|-------|-------------|
| | | • hostName<br>• vendor<br>• model<br>• version<br>• users - Logged on users using this IP info obtained from Active Directory<br>    • userName - Active Directory login name<br>    • fullName - Full name of this user in Active Directory or defined manually<br>    • email - email address of the user in Active Directory or defined manually<br>    • jobTitle - jobTitle of the user in Active Directory or defined manually<br>    • First and last seen times for this IP address to user binding |

## Notification via SNMP Trap

FortiSIEM can also send out SNMP traps when an incident triggers. Use the MIB file (available here) to configure your device to handle SNMP traps sent from FortiSIEM.

**Release Added**: 5.1

## Notification via API

You can also query for incidents via a REST API.

- Request API Specifications
- Polling API Specifications
- Results API Specifications
- Incident Attribute List
- Incident XML Schema

This REST API based caller makes an HTTP(S) request with an input XML. An output XML is returned. Since the number of returned results can be large, the requester has to first get the total number of results, and then get the results one chunk at a time.

This REST API based caller makes an HTTP(S) request with an input XML that defines the query. Since a query can take some time and the number of returned results can be large, the query works as follows

1. Caller submits the query and gets a Query Id back from FortiSIEM. This is done via Request API.
2. Caller polls for query progress and waits until the query is completed. This is done via Polling API
3. When the query is completed, Caller gets the results via Results API.
   a. Caller gets the total number of query results and the query result fields.
   b. Caller gets the results - one chunk at a time.

## Request API Specifications

| | |
|---|---|
| **Release Added** | 5.1 |
| **Input URL** | `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/query/eventQuery` |
| **Input Parameters** | XML file containing the query parameters |
| **Input Credentials** | • **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments. Curl example: `curl -k -u super/admin:Admin*123` <br> • **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access. Curl example with super organization: `curl -k -u super/admin:Admin*123` If querying for a specific organization, replace "super" with the organization name. |
| **Output** | `queryId` or an error code if there is a problem in handling the query or the query format. |

## Polling API Specifications

The request will poll until the server completes the query.

| | |
|---|---|
| **Release Updated** | 6.7.0 |
| **Input URL** | `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/query/progress/<requestId>,<expireTime>` |
| **Output** | progress (pct) <br> Until progress reaches 100, at which point the server completes the query, you must continue polling the server. This is because the server may need to aggregate the results or insert meta-information before sending the results. |

## Results API Specifications

| | |
|---|---|
| **Release Added** | 5.1 |
| **Input URL** | `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/query/events/<queryId>/<begin>/<end>` |
| **Output** | totalCount (first time) and an XML containing the incident attributes. <br> For the first call, **begin** = 0 and **end** can be 1000. You must continuously query the server by using the same URL, but increasing the `begin` and `end` until the totalCount is reached |

# Incident Attribute List

```
bizService,eventType,phCustId,incidentClearedReason,incidentTicketStatus,incidentLastSe
en,eventSeverity,incidentTicketUser,hostIpAddr,eventName,phEventCategory,incidentTicket
Id,count,incidentDetail,incidentSr
c,eventSeverityCat,incidentFirstSeen,incidentViewUsers,incidentComments,incidentCleared
User,incidentNoti
Recipients,incidentId,phRecvTime,incidentStatus,incidentViewStatus,incidentTarget,incid
entRptIp
```

# Incident Notification XML Schema

The following is the schema for incident notification output file:

```xml
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:element name="incident">
<xs:complexType>
<xs:sequence>
        <xs:element type="xs:string" name="name"/>
        <xs:element type="xs:string" name="description"/>
        <xs:element type="xs:string" name="displayTime"/>
        <xs:element type="xs:string" name="incidentSource"/>
        <xs:element name="incidentTarget">
                <xs:complexType>
                        <xs:sequence>
                                <xs:element name="entry">
                                <xs:complexType>
                                <xs:simpleContent>
                                        <xs:extension base="xs:string">
                                        <xs:attribute type="xs:string" name="attribute"/>
                                        <xs:attribute type="xs:string" name="name"/>
                                </xs:extension>
                                </xs:simpleContent>
                        </xs:complexType>
                </xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="incidentDetails">
<xs:complexType>
<xs:sequence>
<xs:element name="entry"> <xs:complexType>
                <xs:simpleContent>
                        <xs:extension base="xs:float">
                                <xs:attribute type="xs:string" name="attribute"/>
                                        <xs:attribute type="xs:string" name="name"/>
                                                </xs:extension>
                                                </xs:simpleContent>
                                                </xs:complexType>
                                        </xs:element>
                                </xs:sequence>
                        </xs:complexType>
                        </xs:element>
```

```
                    <xs:element type="xs:string" name="affectedBizSrvc"/>
                    <xs:element type="xs:string" name="identityLocation"/>
            </xs:sequence>
            <xs:attribute type="xs:short" name="incidentId"/>
            <xs:attribute type="xs:string" name="ruleType"/>
            <xs:attribute type="xs:byte" name="severity"/>
            <xs:attribute type="xs:byte" name="repeatCount"/>
            <xs:attribute type="xs:string" name="organization"/>
            <xs:attribute type="xs:string" name="status"/>
        </xs:complexType>
        </xs:element>
</xs:schema>
```

Refer to Example Usage for incident notification via API.

# Get Triggering Event IDs for One or More Incidents

This API enables you to get the triggering event IDs for one or more incidents

## API Specifications

| | |
|---|---|
| **Release Added** | 5.2.5 |
| **Methodology** | REST API based: Caller makes an HTTPS request with query parameter: `incidentId`. |
| **Request URL** | `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/incident/` `triggeringEvents?incidentIds=<incidentId1>,<incidentId2>` |
| **Input Credentials** | • **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.<br>Curl example: `curl -k -u super/admin:Admin*123`<br>• **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.<br>Curl example with super organization: `curl -k -u super/admin:Admin*123`<br>If querying for a specific organization, replace "super" with the organization name. |
| **Input Parameters** | Query parameters: `incidentIds` |
| **Output** | XML that contains the triggered event IDs for all incidents in the input list. |

Refer to Example Usage to get the list of monitored devices and attributes.

# Update Incident Attributes

This API enables you to update certain incident attributes.

| | |
|---|---|
| **Release Added** | 5.2.5 |
| **Methodology** | REST API based: Caller makes an HTTPS request with an input JSON containing the updated incident attributes |
| **Request URL** | `https://<FortiSIEM_Supervisor_IP>/phoenix` `/rest/incident/external` |
| **Input Credentials** | • **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments. <br> Curl example: `curl -k -u super/admin:Admin*123` <br><br> • **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access. <br> Curl example with super organization: `curl -k -u super/admin:Admin*123` <br> If querying for a specific organization, replace "super" with the organization name. |
| **Input JSON** | **ContentType:** `application/json` <br><br> **RequestPayload:** <br> `{"incidentId":"1","comments":"XYZ","incidentStatus":` `"3","externalTicketType":"MEDIUM","externalTicketId":` `"1111","externalTicketState":"CLOSED",` `"externalAssignedUser":"ABC"}` <br><br> • `incidentId` – Incident ID for the incident to be updated <br> • `comments` – Any comments <br> • `incidentStatus` – 0 (Active), 1 (Auto Cleared), 2 (Manually Cleared), or 3 (System Cleared) <br> • `externalTicketType` – Low, Medium, or High <br> • `externalTicketId` – External Ticket ID <br> • `externalTicketState` – New, Assigned, In Progress, or Closed <br> • `externalAssignedUser` – External Assigned User |
| **Output** | HTTP status code |

Refer to Example Usage to get the list of monitored devices and attributes.

# JSON API Incident Integration

These JSON REST APIs allow you to integrate incidents from FortiSIEM. This is used for ServiceNow SecOps integration.

- Fetch Incidents
- Fetch Trigger Events

- Update Incidents
- Integer Field Mapping to Description

A list of FortiSIEM Incident attributes can be found here.

Refer to Example Usage for Incident Integration examples.

## Fetch Incidents

This API retrieves incidents from FSIEM database.

**Release Added**: 6.3.0

| URI | Method | Additional Information |
|---|---|---|
| /phoenix/rest/pub/incident | GET | **Parameters**<br>"status": [0],<br>* "incidentId":[8064],<br>* "timeFrom": 1620677781736, (Required)<br>* "timeTo": 1620684981736, (Required)<br>* "start":0,(optional)<br>* "size": 500 (by default, return 500 incidents each time) |
| /phoenix/rest/pub/incident | POST | **Payload:**<br><br>```<br>{<br>    "filters": {<br>            " status": [0],<br>             "incidentId":[8064]<br>},<br>"start":0,(optional)<br>"size":500,(by default, return 500 incidents each time)<br>    "timeFrom": 1620677781736, (Required if incidentId is not specified)<br>"timeTo": 1620684981736, (Required if incidentId is not specified)<br>    "orderBy": "incidentLastSeen", (this field must be in the list of fields)<br>    "descending": true,<br>   "fields": [<br>        "eventSeverityCat",<br>        "eventSeverity",<br>        "incidentLastSeen",<br>        "incidentFirstSeen",<br>        "eventType",<br>``` |

| URI | Method | Additional Information |
|---|---|---|

```
                                    "eventName",
                                    "incidentSrc",
                                    "incidentTarget",
                                    "incidentDetail",
                                    "incidentRptIp",
                                    "incidentRptDevName",
                                    "incidentStatus",
                                    "incidentComments",
                                    "customer",
                                    "incidentClearedReason",
                                    "incidentClearedTime",
                                    "incidentClearedUser",
                                    "count",
                                    "incidentId",
                                    "incidentSrc",
                                    "incidentTarget",
                                    "incidentExtUser",
                                    "incidentExtClearedTime",
                                    "incidentExtTicketId",
                                    "incidentExtTicketState",
                                    "incidentExtTicketType",
                                    "incidentReso",
                                    "phIncidentCategory",
                                    "phSubIncidentCategory",
                                    "incidentTitle",
                                    "attackTechnique",
                                    "attackTactic"
                                ]
                            }
```

**Returns:**

```
{
    "total": 317,
   "start":0,
    "size": 10,
    "data": [
           {
                "incidentTitle": "SNMP service down on
wk5794.fortinet.com",
                "eventSeverity": 10,
                "incidentFirstSeen": 1621941030000,
                "incidentReso": 1,
                "incidentRptIp": "172.30.57.94",
                "incidentLastSeen": 1621987770000,
```

| URI | Method | Additional Information |
|---|---|---|

```
                                       "incidentSrc": "",
                                       "count": 54,
                                       "attackTechnique": "[{\"name\": \"Service
                             Stop\", \"techniqueid\": \"T1489\"}]",
                                       "eventType": "PH_RULE_SNMP_DOWN",
                                       "phIncidentCategory": 1,
                                       "incidentClearedTime": 0,
                                       "incidentTarget": "hostIpAddr:172.30.57.94,
                             hostName:wk5794.fortinet.com,",
                                       "attackTactic": "Impact",
                                       "eventSeverityCat": "HIGH",
                                       "incidentDetail": "",
                                       "incidentRptDevName":
                             "wk5794.fortinet.com",
                                       "eventName": "SNMP Service Unavailable",
                                       "incidentId": 114780,
                                       "incidentStatus": 0,
                                       "customer": "Super"
                                   },
                                 . ..
                             ]
                             }
```

## Fetch Trigger Events

This API retrieves triggering events from incidents.

**Release Added**: 6.3.0

| URI | Method | Additional Information |
|---|---|---|
| /phoenix/rest/pub/incident/triggeringEvents?incidentId=8&size=10 | GET | **Parameters**:<br>incidentId: FortiSIEM incident Id (Required) size: indicates how many trigger events return, 10 events by default if no size specific.<br>**Returns**:<br><br>`[`<br>`    {`<br>`        "custId": 1,`<br>`        "index": 0,` |

| URI | Method | Additional Information |
|---|---|---|
| | | "id": 6482650188627892000,<br>        "eventType": "PH_DEV_ MON_PERFMON_JOB_DELAY_HIGH",<br>        "receiveTime": 1621557630000,<br>        "rawMessage": "<174>May 20 17:40:30 [PH_ DEV_MON_PERFMON_JOB_DELAY_ HIGH]:[jobName]=CPU Util (SNMP),[phCustId]=1, [hostName]=FGT50E3U17000553, [eventSeverity]=PHL_INFO, [phEventCategory]=3, [hostIpAddr]=172.30.58.50, [procName]=AppServer, [relayDevName]=sp5875, [relayDevIpAddr]=172.30.58.7 5,[phLogDetail]=A performance metric delay for a single device crossed high water mark",<br>        "nid": "6482650188627892238",<br>        "attributes": {<br>            "1": "PH_DEV_MON_ PERFMON_JOB_DELAY_HIGH",<br>            "2": 1,<br>            "7": 1621557630000,<br>            "8": "172.30.58.75",<br>            "9": "172.30.58.75",<br>            "10": "sp5875",<br>            "11": "sp5875",<br>            "12": 1,<br>            "13": "<174>May 20 17:40:30 [PH_DEV_MON_ PERFMON_JOB_DELAY_HIGH]: [jobName]=CPU Util(SNMP), [phCustId]=1, [hostName]=FGT50E3U17000553, [eventSeverity]=PHL_INFO, [phEventCategory]=3, |

| URI | Method | Additional Information |
|---|---|---|
| | | ayDevName]=sp5875,<br>[relayDevIpAddr]=172.30.58.7<br>5,[phLogDetail]=A performance<br>metric delay for a single<br>device crossed high water<br>mark",<br>      "15":<br>6482650188627892000,<br>      "16": 3,<br>      "17": 1,<br>      "21": 1,<br>      "24": "LOW",<br>      "43": "Fortinet",<br>      "44":<br>"FortiSIEM",<br>      "53": "Super",<br>      "110": 1,<br>      "122":<br>"PHBoxParser",<br>      "129": 1,<br>      "1005":<br>"172.30.58.50",<br>      "1006":<br>"FGT50E3U17000553",<br>      "2007":<br>"AppServer",<br>      "4506": "CPU Util<br>(SNMP)"<br>    },<br>    "eventAttributes": [<br>],<br>    "dataStr": { }<br>  }<br>] |

## Update Incidents

This API allows you to update incident ticket status.

**Release Added**: 6.3.0

| URI | Method | Additional Information |
|---|---|---|
| /phoenix/rest/pub/incident/update/<br>{*incidentId*} | POST | **Parameter**:<br>IncidentId: FortiSIEM incident Id (Required)<br>**Payload**: |

| URI | Method | Additional Information |
|---|---|---|
| | | `{`<br>`    "incidentExtUser":"User A",`<br>`    "incidentExtClearedTime":1620677781736,`<br>`(Timestamp)`<br>`    "incidentExtTicketId":"INS00456",`<br>`(Required)`<br>`    "incidentExtTicketState":"Closed",`<br>`    "incidentExtTicketType":""`<br>`}` |

# Integer Field Mapping to Descriptions

## Incident Status

"incidentStatus":,

ACTIVE = 0;

AUTOMATICALLY CLEARED = 1;

MANUALLY CLEARED = 2;

SYSTEM CLEARED = 3

## Incident Resolution

"incidentReso":

None = 0

Open = 1

TruePositive = 2

FalsePositive = 3

InProgress = 4

## Incident Category

"phIncidentCategory":,

AVAILABILITY = 1;

PERFORMANCE = 2;

CHANGE = 3;

SECURITY = 4;

OTHER = 5;

# FortiSIEM Incident Attributes List

"eventSeverityCat",

"eventSeverity",

"incidentLastSeen",

"incidentFirstSeen",

"eventType",

"eventName",

"incidentSrc",

"incidentTarget",

"incidentDetail",

"incidentRptIp",

"incidentRptDevName",

"incidentStatus",

"incidentComments",

"customer",

"incidentClearedReason",

"incidentClearedTime",

"incidentClearedUser",

"count",

"incidentId",

"incidentExtUser",

"incidentExtClearedTime",

"incidentExtTicketId",

"incidentExtTicketState",

"incidentExtTicketType",

"incidentReso",

"phIncidentCategory",

"phSubIncidentCategory",

"incidentTitle",

"attackTechnique",

"attackTactic"

# Lookup Table Integration

The following Lookup Table Integration APIs are available:

- POST pub/lookupTable
- GET pub/lookup Table
- DELETE pub/lookupTable/{*lookupTableId*}
- POST pub/lookupTable/{*lookupTableId*}/import
- GET pub/lookupTable/{*lookupTableId*}/task/{*taskId*}
- GET pub/lookupTable/{*lookupTableId*}/data
- PUT pub/lookupTable/{*lookupTableId*}/data
- PUT pub/lookupTable/{*lookupTableId*}/data/delete

# POST pub/lookupTable

## LookupTable - Post

The LookupTable endpoint allows you to create the definition of a lookupTable.

**Release Added**: 6.4.0

## Resource

POST /pub/lookupTable

## Authorization

Basic access authentication

## Post Parameters

| Name | Type | Description |
|---|---|---|
| name | string | The lookup table name. |
| description | string | Description of the lookup table. |
| custID | integer | The Organization ID: id of the organization on which to create the lookup table. To |

| Name | Type | Description |
|------|------|-------------|
| (optional) | | retrieve this ID, navigate to **ADMIN > Setup > Organizations**, and refer to the **ID** column. |
| columnList[] | array | The list of column definitions of the lookup table. |
| columnList [].key | boolean | Whether the primary column is key. |
| columnList [].name | string | The column name. |
| columnList [].type | string | The column type, which can be STRING, LONG, or DOUBLE |

## Example

```
{
  "name": "csurl_scores",
  "description": "",
  "organizationName": "Super",
  "columnList": [
    {
      "key": true,
      "name": "url",
      "type": "STRING"
    },
    {
      "key": false,
      "name": "wfCategoryID",
      "type": "LONG"
    },
    {
      "key": false,
      "name": "score",
      "type": "DOUBLE"
    }
  ]
}
```

## Response

Status-Code: 200 OK

```
{
  "id": 1250451,
  "name": "csurl_scores",
  "description": "",
  "organizationName": "Super",
```

```
    "columnList": [
      {
        "key": true,
        "name": "url",
        "type": "STRING"
      },
      {
        "key": false,
        "name": "wfCategoryID",
        "type": "LONG"
      },
      {
        "key": false,
        "name": "score",
        "type": "DOUBLE"
      }
    ]
  }
```

## HTTP Error Codes

| HTTP Status | Code | Description |
|---|---|---|
| 401 | unauthorized | The bearer credential is invalid. |
| 400 | bad request | The request made is incorrect or corrupt. |
| 422 | missing parameters | Parameters are missing in query/request body. |
| 423 | invalid parameters | The parameters are invalid in path/query/request body. |

# GET pub/lookup Table

## LookupTable - Get

The LookupTable endpoint lets you retrieve the list of lookupTable definitions.

**Release Added**: 6.4.0

## Resource

GET /pub/lookupTable

## Authorization

Basic access authentication

## Query Parameters

| Name | Type | Description |
|---|---|---|
| status (optional) | integer | Offset the list of returned results by this amount. Default is zero. |
| size (optional) | integer | Number of items to retrieve. Default is 25, maximum is 1000. |

## Example Request

Replace <*credentials*> in the example below with the Base64 encoding of username and password joined by a single colon :

```
curl -H 'Authorization: Basic <credentials>' \
     -H 'content-type: application/json' \
     'https://<IP>/phoenix/rest/pub/lookupTable'
```

## Response

Status-Code: 200 OK

```
{
  "data": [
    {
      "columnList": [
        {
          "key": true,
          "name": "url",
          "type": "STRING"
        },
        {
          "key": false,
          "name": "wfCategoryID",
          "type": "LONG"
        },
        {
          "key": false,
          "name": "score",
          "type": "DOUBLE"
        }
      ],
      "organizationName": "Super",
      "description": "",
      "id": 1250451,
      "lastUpdated": 1632432976253,
      "lastUpdatedResult": "importDataViaFile : 24181 rows are imported successful.",
      "name": "csurl_scores"
    }
  ],
  "total": 1,
  "start": 0,
  "size": 25
}
```

## Request Parameters

| Name | Type | Description |
|------|------|-------------|
| total | string | Total number of items. |
| start | integer | Position in pagination. |
| size | integer | Number of items to retrieve. |
| data | array | An array of lookup Table definition. |
| data[].id | integer | The lookup Table ID. |
| data[].organizationName | integer | The organization name. |
| data[].name | string | The lookup Table name. |
| data[].description | string | The description of the lookup Table. |
| data[].lastUpdated | integer | Unix timestamp when the last update of the lookup Table content occurred. |
| data[].lastUpdatedResult | string | The result of the last updated lookup Table content. |
| data[].columnList[] | array | The list of column definitions of the lookup Table. |
| data[].columnList[].key | boolean | Whether it is the primary column key. |
| data[].columnList[].name | string | The column name. |
| data[].columnList[].type | string | The column type, which can be STRING, LONG, or DOUBLE. |

## HTTP Error Codes

| HTTP Status | Code | Description |
|-------------|------|-------------|
| 401 | unauthorized | The bearer credential is invalid. |
| 400 | bad request | The request made is incorrect or corrupt. |
| 422 | missing parameters | Parameters are missing in query/request body. |
| 423 | invalid parameters | The parameters are invalid in path/query/request body. |

# DELETE pub/lookupTable/{*lookupTableId*}

## LookupTable - Delete

The LookupTable endpoint allows you to delete the lookupTable definition.

**Release Added**: 6.4.0

## Resource

DELETE /pub/lookupTable/{*lookupTableId*}

## Authorization

Basic access authentication

## Path Parameters

| Name | Type | Description |
|------|------|-------------|
| lookupTableId | integer | Unique identifier representing the lookup Table. |

## Query Parameters

None

## Example Request

```
curl -H 'Authorization: Basic <credentials>' \
    -H 'content-type: application/json' \
    -X DELETE \
    'https://<IP>/phoenix/rest/pub/lookupTable/<lookupTableId>'
```

## Response

Status-Code: 204 No Content

# POST pub/lookupTable/{*lookupTableId*}/import

## LookupTable import data - Post

The LookupTable endpoint allows importing the data of lookupTable.

**Release Added**: 6.4.0

## Resource

POST /pub/lookupTable/{*lookupTableId*}/import

## Authorization

Basic access authentication

## Post Parameters

Content-Type: multipart/form-data

| Name | Type | Description |
|------|------|-------------|
| file | file | CSV file. |
| mapping | string | The configuration matches the position of columns in the CSV file to columns in lookup Table. Format as below:<br><br>`{`<br>`    "<LookupTable_Column_Name_1>":<Position_1>,`<br>`"<LookupTable_Column_Name_2>":<Position_2>,`<br>`......`<br>`}`<br><br>*<LookupTable_Column_Name_1>*: string<br>*<Position>*: integer (from 1)<br><br>`{`<br>`    "url":1,`<br>`    "wfCategoryID":2`<br>`}` |
| fileSeparator (optional) | string | The csv file separator. Default is the comma character, ",". |
| fileQuoteChar (optional) | string | The csv file quote character. Default is the double quotation character, """. |
| skipHeader (optional) | boolean | Whether to ignore the csv file header. Default is false. |
| updateType (optional) | string | Data update type. Either "Overwrite" or "Append". Default is "Overwrite". |

## Example Request

```
curl -H 'Authorization: Basic <credentials>' \
    -X POST \
    'https://<IP>/phoenix/rest/pub/lookupTable/<lookupTableId>/import'
    -F 'file=@"/<FileDir>/<FileName>.csv"' \
    -F 'mapping="{\"url\":1,\"wfCategoryID\":2}"' \
    -F 'fileSeparator=","' \
```

```
-F 'fileQuoteChar="\""' \
-F 'skipHeader="true"'
```

## Response

Content-Type: application/json

Status-Code: 200 OK

```
{
  "taskId": 1250
}
```

| Name | Type | Description |
|------|------|-------------|
| taskId | long | The task id of importing data to the lookupTable. |

## HTTP Error Codes

| HTTP Status | Code | Description |
|-------------|------|-------------|
| 401 | unauthorized | The bearer credential is invalid. |
| 400 | bad request | The request made is incorrect or corrupt. |
| 422 | missing parameters | Parameters are missing in query/request body. |
| 423 | invalid parameters | The parameters are invalid in path/query/request body. |

# GET pub/lookupTable/{*lookupTableId*}/task/{*taskId*}

## LookupTable check importing task status - Get

The LookupTable endpoint allows checking the status of import data.

**Release Added**: 6.4.0

## Resource

GET /pub/lookupTable/{*lookupTableId*}/task/{*taskId*}

## Authorization

Basic access authentication

## Path Parameters

| Name | Type | Description |
|------|------|-------------|
| lookupTableId | integer | The lookup Table Id. |
| taskId | integer | The task id of the importing data to the lookup Table. It is retrieved from the Import API response. |

## Example Request

Replace *<credentials>* in the example below with the Base64 encoding of username and password joined by a single colon :

```
curl -H 'Authorization: Basic <credentials>' \
     -H 'content-type: application/json' \
     'https://<IP>/phoenix/rest/pub/lookupTable/<lookupTableId>/task/<taskId>'
```

## Response

Status-Code: 200 OK

```
{
  "id": 1250
  "status": "Done",
  "progress": 100,
  "actionResult": "557 rows are imported successful."
}
```

| Name | Type | Description |
|------|------|-------------|
| id | integer | The id of task. |
| status | string | The status of task. |
| progress | integer | The progress of task. |
| actionResult | string | The action result of import data task. |

## HTTP Error Codes

| HTTP Status | Code | Description |
|-------------|------|-------------|
| 401 | unauthorized | The bearer credential is invalid. |
| 400 | bad request | The request made is incorrect or corrupt. |

# GET pub/lookupTable/*{lookupTableId}*/data

## Query LookupTable Data - Get

The LookupTable endpoint allows retrieving items of lookupTable.

**Release Added**: 6.4.0

## Resource

GET /pub/lookupTable/*{lookupTableId}*/data

## Authorization

Basic access authentication

## Query Parameters

| Name | Type | Description |
|---|---|---|
| start (optional) | integer | Offset the list of returned results by this amount. Default is zero. |
| size (optional) | integer | Number of items to retrieve. Default is 25, maximum is 1000. |
| searchText (optional) | string | Search text. |
| sortBy (optional) | string | Sorted by one of lookupTable columns with descending order. Format: *<ColumnName><A blank space><ACS or DESC for ascending or descending order respectively>* |

## Example Request

Replace *<credentials>* in the example below with the Base64 encoding of username and password joined by a single colon :

```
curl -H 'Authorization: Basic <credentials>' \
     -H 'content-type: application/json' \
'https://<
IP
>/phoenix/rest/pub/lookupTable/<
lookupTableId>/data?size=25&start=0&searchText=example&sortBy=score%20acs>'
```

# Response

Status-Code: 200 OK

```
{
  "data": [
    {
      "url": "http://example.com",
      "wfCategoryID": 26,
      "score": 0.20050119
    },
    {
      "url": "http://www.sample.com/wp-login.php",
      "wfCategoryID": 26,
      "score": 0.25293878
    },
    {
      "url": "http://www.instance.com/case1",
      "wfCategoryID": 26,
      "score": 0.25635383
    },
    {
      "url": "http://www.instance.com/case2",
      "wfCategoryID": 26,
      "score": 0.25635383
    }
  ],
  "total": 4,
  "start": 0,
  "size": 25
}
```

| Name | Type | Description |
|------|------|-------------|
| total | string | Total number of items. |
| start | integer | Position in pagination. |
| size | integer | Number of items to retrieve (1000 max). |
| data | array | An array of lookup Table items. Each item is a dictionary which contains lookupTable column name and its value. |

# HTTP Error Codes

| HTTP Status | Code | Description |
|-------------|------|-------------|
| 401 | unauthorized | The bearer credential is invalid. |
| 400 | bad request | The request made is incorrect or corrupt. |
| 422 | missing parameters | Parameters are missing in query/request body. |
| 423 | invalid parameters | The parameters are invalid in path/query/request body. |

# PUT pub/lookupTable/*{lookupTableId}*/data

## Update LookupTable Data - PUT

The LookupTable endpoint allows updating the item of lookupTable.

**Release Added**: 6.4.0

## Resource

PUT /pub/lookupTable/{*lookupTableId*}/data

## Authorization

Basic access authentication

## Path Parameters

| Name | Type | Description |
|------|------|-------------|
| lookupTableId | integer | Unique identifier representing the lookup Table. |

## Query Parameters

| Name | Type | Description |
|------|------|-------------|
| key | map | The primary key of item column and its value. Format: {"*<keyColumn_1>*":*<value>*} <br><br> `key={"url":"http://example.com"}` |

## Example Request

Replace *<credentials>* in the example below with the Base64 encoding of username and password joined by a single colon :

```
curl -g -H 'Content-Type: application/json' \
    -H 'Authorization: Basic <credentials>' \
    -X PUT \
'https://<IP>/phoenix/rest/pub/lookupTable/<lookupTableId>/data?key=
{%22url%22:%20%22http://example.com%22}' \
    --data-raw \
    '{
        "url": "www.test.com",
        "wfCategoryID": 30,
```

```
        "score": 0.50119
    }'
```

## PUT Body

```
{
  "url": "http://test.com"
  "wfCategoryID": 30,
  "score": 0.50119
}
```

| Name | Type | Description |
|------|------|-------------|
| *<LookupTableColumnName>* | string | Column name. |
| *<value>* | string, integer, double | Value. |

## Response

Status-Code: 200 OK

## HTTP Error Codes

| HTTP Status | Code | Description |
|-------------|------|-------------|
| 401 | unauthorized | The bearer credential is invalid. |
| 400 | bad request | The request made is incorrect or corrupt. |
| 422 | missing parameters | Parameters are missing in query/request body. |
| 423 | invalid parameters | The parameters are invalid in path/query/request body. |

# PUT pub/lookupTable/{*lookupTableId*}/data/delete

## Delete LookupTable Data- PUT

The LookupTable endpoint allows deleting the lookupTable item.

**Release Added**: 6.4.0

## Resource

PUT /pub/lookupTable/{*lookupTableId*}/data/delete

## Authorization

Basic access authentication

## Path Parameters

| Name | Type | Description |
|------|------|-------------|
| lookupTableId | integer | Unique identifier representing the lookup Table. |

## Post Parameters

| Name | Type | Description |
|------|------|-------------|
| *&lt;array&gt;* | list | List of primary key and value map. |
| *&lt;map&gt;* | map | The primary key of item column and its value. Format: {"*&lt;keyColumn_1&gt;*":*&lt;value&gt;*} <br> {"url":"http://example.com"} |

## Example Request

```
curl -g -H 'Content-Type: application/json' \
     -H 'Authorization: Basic <credentials>' \
     -X PUT \
'https://<IP>/phoenix/rest/pub/lookupTable/<lookupTableId>/data/delete' \
     --data-raw \
'[
    {
            "url": "http://www.sample.com/wp-login.php"
        },
    {
            "url": "http://www.instance.com/case1"
        },
    {
            "url": "http://www.sample.com/case2"
        }
    ]'
```

## Response

Status-Code: 204 No Content

## HTTP Error Codes

| HTTP Status | Code | Description |
| --- | --- | --- |
| 401 | unauthorized | The bearer credential is invalid. |
| 400 | bad request | The request made is incorrect or corrupt. |
| 422 | missing parameters | Parameters are missing in query/request body. |
| 423 | invalid parameters | The parameters are invalid in path/query/request body. |

# Performance and Health API

The following GET APIs are available for retrieving health summary and health details of FortiSIEM Manger and the FortiSIEM Instances which are registered to the FortiSIEM Manager.

- Get Health Summary
- Get Health Details by Instance Id
- Get Health Details - Complete Response

## Get Health Summary

This API can be run against the Supervisor of a single FortiSIEM instance or against FortiSIEM Manager.

- Single Instance Supervisor returns the health *summary* of the Supervisor, Workers and Collectors in that FortiSIEM Instance.
- FortiSIEM Manager returns the health *summary* of FortiSIEM Manager and all the FortiSIEM instances registered to that FortiSIEM Manager.

**Release Added**: 6.5.0

| | |
|---|---|
| **Input URL (FortiSIEM Supervisor)** | `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/system/health/summary` |
| **Input URL (FortiSIEM Manager)** | `https://<FortiSIEM_Manager_IP>/phoenix/rest/system/health/summary` |

### Input Credentials

- **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.
  Curl example: `curl -k -u super/admin:Admin*123`
- **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.
  Curl example with super organization: `curl -k -u super/admin:Admin*123`
  If querying for a specific organization, replace "super" with the organization name.

### HTTP Method

GET

### Output

When the request succeeds (HTTP response code 200), a JSON file is returned with all information included.

The Instance health summary returned by Single Instance Supervisor includes the health summary of the Supervisor, all Workers, and Collectors. If the health of a node is anything other than normal, then the offending metric indicator is also included. See File1_InstanceHealthSummaryExample.txt.

The health summary returned by FortiSIEM Manager includes the health summary of all registered Instances and FortiSIEM Manager itself. The health summary of a registered FortiSIEM instance includes the health summary of the Supervisor, all Workers, and Collectors in that Instance. If the health of a node is anything other than normal, then the offending metric indicator is also included. See File2_ManagerHealthSummaryExample.txt.

Health is based on the following.

- Generic metrics – CPU, Load average, Memory, Swap, Disk space, Disk I/O, Process Uptime/CPU/Memory
- Supervisor specific metrics – NFS I/O, Shared Store pointers
- Worker specific metrics – Worker Upload Queue, NFS I/O, Shared Store pointers, Last Status Update
- Collector Specific metrics – Event Upload Queue, Last Status Update, Last File Received, Last Event Received

The health metrics are defined in Appendix - Description of Health JSON Attributes. The thresholds used to determine normal/warning/critical status are in Appendix - Current Thresholds for Health Status. Note that only the latest values are returned by the API.

# Get Health Details by Instance Id

This API provides complete health information of specific FortiSIEM instance with given Instance Id. The instance Id can be obtained from running the Get Health Summary API.

**Release Added**: 6.5.0

| | |
|---|---|
| **Input URL** | `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/system/health/instance?instanceId=<instance_id>` |

## Input Credentials

- **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.
  Curl example: `curl -k -u super/admin:Admin*123`
- **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.
  Curl example with super organization: `curl -k -u super/admin:Admin*123`
  If querying for a specific organization, replace "super" with the organization name.

## HTTP Method

GET

## Request Path Parameter

| Field | Description |
|---|---|
| Replace *<instance_id>* with long value | Instance id of specific instance |

## Output

When the request succeeds (HTTP response code 200), a JSON file is returned with the following.

- Health metrics of each node (including Super, Workers and Collectors)
- Health assessment of each node

See File3_InstanceHealth_DetailsExample.txt for an example.

Health metrics includes the following.

- Generic metrics – CPU, Load average, Memory, Swap, Disk space, Disk I/O, Process Uptime/CPU/Memory, EPS
- Supervisor specific metrics – NFS I/O, Shared Store pointers
- Worker specific metrics – Worker Upload Queue, NFS I/O, Shared Store pointers, Last Status Update
- Collector Specific metrics – Event Upload Queue, Last Status Update, Last File Received, Last Event Received

The health metrics are defined in Appendix - Description of Health JSON Attributes. The thresholds used to determine normal/warning/critical status are in Appendix - Current Thresholds for Health Status. Note that only the latest values are returned by the API.

# Get Health Details – Complete Response

This API returns the complete health information of FortiSIEM Manager and all FortiSIEM nodes belonging to each FortiSIEM Instance registered to the FortiSIEM Manager. This can be quite large depending on the number of registered instances and the number of nodes in each instance.

**Release Added**: 6.5.0

**Input URL**  `https://<FortiSIEM_Manager_IP>/phoenix/rest/system/health`

## Input Credentials

- **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.
  Curl example: `curl -k -u super/admin:Admin*123`
- **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.
  Curl example with super organization: `curl -k -u super/admin:Admin*123`
  If querying for a specific organization, replace "super" with the organization name.

# HTTP Method

GET

# Output

When the request succeeds (HTTP response code 200), a JSON file is returned with the following.

- Health metrics of FortiSIEM Manager and each Super/Worker/Collector node in every registered Instance
- Health assessment of each node

See File4_ManagerHealth_DetailsExample.txt for an example.

Health metrics includes the following.

- Generic metrics – CPU, Load average, Memory, Swap, Disk space, Disk I/O, Process Uptime/CPU/Memory, EPS
- Supervisor specific metrics – NFS I/O, Shared Store pointers
- Worker specific metrics – Worker Upload Queue, NFS I/O, Shared Store pointers, Last Status Update
- Collector Specific metrics – Event Upload Queue, Last Status Update, Last File Received, Last Event Received

The health metrics are defined in Appendix - Description of Health JSON Attributes. The thresholds used to determine normal/warning/critical status are in Appendix - Current Thresholds for Health Status. Note that only the latest values are returned by the API.

# REST API to Return Worker Queue State

The following public REST API can be used to query Worker Event Upload Queue state. An upstream load balancer can use the information to route events from Collectors to the least loaded Worker.

**Release Added**: 6.4.0

API: `GET https://<Worker_IP>/workerUploadHealth/response.json`

Response: `{ allowUpload: true, fileQueueSizeMB: 500, fileQueueCount: 300 }`

| Response Parameter | Description |
|---|---|
| allowUpload | True means Worker upload queue is less than 100MB and Worker will accept events.<br>False means Worker upload queue is more than 100MB and Worker will reject events. This is likely because inserts to event database is slow. |
| fileQueueSizeMB | Current file queue size in MB. |
| fileQueueCount | Current file queue count. |

# Watchlist Integration

The Watchlist Integration APIs are broken down into the following sections:

- Read APIs for Integration with FortiGate Firewalls
  - Get IPs
  - Get Domains
  - Get Hash
- Generic Read APIs
  - Get All Watch Lists
  - Get Watch List Entries Count
  - Get Watch List by Watch List ID
  - Get Watch List by Watch List Entry Value
  - Get Watch List by Watch List Entry ID
  - Get Watch List Entry by Watch List Entry ID
- Update APIs
  - Update State of Watch List Entry by Watch List Entry ID
  - Update State of Watch List Entry by Watch List Entry Value
  - Update Last Seen Time of Watch List Entry by Watch List Entry ID
  - Update Last Seen Time of Watch List Entry by Watch List Entry Value
  - Update Count of Watch List Entry by Watch List Entry ID
  - Update Count of Watch List Entry by Watch List Entry Value
  - Add Watch List Entry(s) to Watch List Groups
  - Save Watch List Groups with Watch List Entry(s)
  - Update Specific Watch List Entry
- Delete APIs
  - Delete Watch List Entry by ID
  - Delete Watch List by ID
- JSON Object Formats
  - Watch List Entry JSON
  - Watch List JSON

Refer to Example Usage for Watchlist Integration examples.

## Read APIs for Integration with FortiGate Firewalls

The following Read APIs return the content in a simplified way to make it easy for the requestor to process the results. FortiGate firewalls can use these APIs natively as a threat feed (For details, see FortiGate/FortiOS Cookbook Threat feeds).

- GET IPs
- GET Domains
- GET Hash

## Get IPs

Use this GET API to retrieve list of watch list IPs with given watch list name. For use with FortiGate.

**Release Added**: 6.6.0

| Input URL | https://*<FortiSIEM_Supervisor_IP>*/phoenix/rest/watchlist/ip?name=*<watchlist_name>* |

### Input Credentials

- **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.
  Curl example: `curl -k -u super/admin:Admin*123`
- **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.
  Curl example with super organization: `curl -k -u super/admin:Admin*123`
  If querying for a specific organization, replace "super" with the organization name.

### Request Path Parameter

| Field | Type | Description |
|-------|------|-------------|
| Name | String | Watch list name |

### Output

| Response Status | Response |
|-----------------|----------|
| Success: When the request succeeds (HTTP response code 200), an empty set or a list of list separated IPs is returned. | Example:<br>`10.0.0.1`<br>`145.12.14.75`<br>`172.30.58.10` |
| Error: When the request fails (HTTP response code not 200). | 1. Response contains failed reason. Example: Wrong watchlist name error.<br>`{"response":"DyWatchList@DNS was not found","status":"Failed"}`<br>2. Response empty. |

# Get Domains

Use this GET API to retrieve list of watch list domains with given watch list name. For use with FortiGate.

**Release Added**: 6.6.0

**Input URL** https://*<FortiSIEM_Supervisor_IP>*/phoenix/rest/watchlist/domain?name=*<watchlist_name>*

## Input Credentials

- **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.
  Curl example: `curl -k -u super/admin:Admin*123`
- **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.
  Curl example with super organization: `curl -k -u super/admin:Admin*123`
  If querying for a specific organization, replace "super" with the organization name.

## Request Path Parameter

| Field | Type | Description |
|-------|------|-------------|
| Name | String | Watch list name |

## Output

| Response Status | Response |
|-----------------|----------|
| Success: When the request succeeds (HTTP response code 200), empty set or a list of list separated domains is returned | Example:<br>`Google.com`<br>`Fortinet.com`<br>`Host.fsm-ip.com` |
| Error: When the request fails (HTTP response code not 200). | 1. Response contains failed reason. Example: Wrong watchlist name error.<br>`{"response":"DyWatchList@DNS was not found","status":"Failed"}`<br>2. Response empty. |

# Get Hash

Use this GET API to retrieve list of Hash (only MD5, SHA1 and SHA256 hash) with given watch list name. For use with FortiGate.

**Release Added**: 6.6.0

**Input URL** https://<*FortiSIEM_Supervisor_IP*>/phoenix/rest/watchlist/hash?name=<*watchlist_name*>

## Input Credentials

- **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. Use "super" as the organization for Enterprise deployments.
  Curl example: `curl -k -u super/admin:Admin*123`
- **Service Provider deployments:** User name and password of Super Global account or Organization specific account and name. Make sure that the account has the appropriate access.
  Curl example with super organization: `curl -k -u super/admin:Admin*123`
  If querying for a specific organization, replace "super" with the organization name.

## Request Path Parameter

| Field | Type | Description |
|-------|------|-------------|
| Name | String | Watch list name |

## Output

| Response Status | Response |
|-----------------|----------|
| Success: When the request succeeds (HTTP response code 200), an empty set or a list of list separated hash (only get MD5, SHA1 and SHA256 hash) is returned. | Example:<br>771ab1c7c8e5c4ad1113ec58a41cc697<br>73e5eb7be756f6264gyy6e8c22ff5x97fb1fab17<br>D4C9D9059326271A89CE57FCAF328ED673F46BE33469FF979E8AB8DD501E554F |
| Error: When the request fails (HTTP response code not 200). | 1. Response contains failed reason.<br>Example: Wrong watchlist name error.<br>`{"response":"DyWatchList@DNS was not found","status":"Failed"}`<br>2. Response empty. |

# Generic Read APIs

These GET APIs are available to retrieve watch lists from the FortiSIEM database.

- Get All Watch Lists
- Get Watch List Entries Count
- Get Watch List by Watch List ID

- Get Watch List by Watch List Entry Value
- Get Watch List by Watch List Entry ID
- Get Watch List Entry by Watch List Entry ID

# Get All Watch Lists

This API retrieves all the watch lists from FSIEM database.

**Release Added**: 6.3.0

| **Input URL** | https://*<FortiSIEM_Supervisor_IP>*/phoenix/rest/watchlist/all |
|---|---|

## Output

| Response Status | Response |
|---|---|
| Success | ```json
{
    "response": [{
        "topGroup": false,
        "entries": [
            {
                "lastSeen": 1613719690008,
                "naturalId": "PVVol_A001_A000356_POWER2_
1613719690011",
                "dataCreationType": "SYSTEM",
                "firstSeen": 1613719690008,
                "count": 10,
                "custId": 1,
                "triggeringRules": "Datastore Space Warning",
                "description": "WL Des",
                "id": 889401,
                "state": "Enabled",
                "entryValue": "PVVol_A001_A000356_POWER2",
                "expiredTime": 0,
                "ageOut": "1d"
            },
            {
                "lastSeen": 1613719690000,
                "naturalId": "PVVol_A001_A000356_POWER2_
1613719690011",
                "dataCreationType": "SYSTEM",
                "firstSeen": 1613719000000,
                "count": 100,
                "triggeringRules": "Datastore Space Warning",
``` |

| Response Status | Response |
|---|---|
| | ```"description": "WL Des Testing again",```<br>```"id": 889402,```<br>```"custId": 1,```<br>```"state": "Disabled",```<br>```"entryValue": "PVVol_A001_A000356_POWER2",```<br>```"expiredTime": 0,```<br>```"ageOut": "10d"```<br>```        }```<br>```    ],```<br>```"isCaseSensitive": null,```<br>```"dataCreationType": null,```<br>```"displayName": "",```<br>```"valueType": "STRING",```<br>```"description": null,```<br>```"id": 0,```<br>```"custId": 1,```<br>```"valuePattern": null,```<br>```"ageOut": null```<br>```},```<br>```            {```<br>```"topGroup": true,```<br>```"entries": null,```<br>```"isCaseSensitive": false,```<br>```"dataCreationType": "USER",```<br>```"displayName": "Test WL Group2",```<br>```"valueType": "STRING",```<br>```"description": "Testing",```<br>```"id": 897300,```<br>```"valuePattern": null,```<br>```"ageOut": "1w"```<br>```    }```<br>```],```<br>```"status": "Success"```<br>```}``` |
| Failure | ```{```<br>```    "response": "Reason for failure",```<br>```    "status": "Failed"```<br>```}``` |

## Get Watch List Entries Count

This API gives the count of watch list entries in any watch list group.

**Release Added**: 6.3.0

| Input URL | https://*<FortiSIEM_Supervisor_IP>*/phoenix/rest/watchlist/cnt |
|---|---|

## Output

| Response Status | Response |
|---|---|
| Success | ```<br>{<br>        "response": {<br>            "entry_count": 6<br>        },<br>        "status": "Success"<br>}<br>``` |
| Failure | ```<br>{<br>        "response": "Reason for failure",<br>        "status": "Failed"<br>}<br>``` |

# Get Watch List by Watch List ID

This API retrieves a specific watch list with given watch list ID.

**Release Added**: 6.3.0

| Input URL | https://<*FortiSIEM_Supervisor_IP*>/phoenix/rest/watchlist/<*watch_list_id*> |
|---|---|

## Request Path Parameter

| Field | Description |
|---|---|
| Replace <*watch_list_id*> with numeric value. | Watch list id of a specific watch list. |

## Output

| Response Status | Response |
|---|---|
| Success | ```<br>{<br>        "response": [<br>            {<br>                "topGroup": true,<br>                "entries": [<br>                    {<br>                        "lastSeen": null,<br>                        "naturalId": "172.30.57.65_<br>1616469746578",<br>                        "dataCreationType": null,<br>                        "firstSeen": null,<br>``` |

| Response Status | Response |
|---|---|
| | ```json<br>            "count": null,<br>            "triggeringRules": null,<br>            "description": "Testing",<br>            "id": 888900,<br>            "custId": 1,<br>            "state": "Enabled",<br>            "entryValue": "172.30.57.65",<br>            "expiredTime": null,<br>            "ageOut": "1w"<br>        },<br>        {<br>            "lastSeen": null,<br>            "naturalId": "PVVol_A001_A000356_<br>POWER23_1616480669538",<br>            "dataCreationType": null,<br>            "firstSeen": null,<br>            "count": null,<br>            "triggeringRules": "Datastore Space<br>Warning",<br>            "description": null,<br>            "id": 889400,<br>            "custId": 1,<br>            "state": "Enabled",<br>            "entryValue": "PVVol_A001_A000356_<br>POWER23",<br>            "expiredTime": null,<br>            "ageOut": "1d"<br>        }<br>    ],<br>    "isCaseSensitive": false,<br>    "dataCreationType": "USER",<br>    "displayName": "Test WL Group",<br>    "valueType": "STRING",<br>    "description": "",<br>    "id": 881750,<br>     "custId": 1,<br>    "valuePattern": null,<br>    "ageOut": "1w"<br>    }<br>  ],<br>  "status": "Success"<br>}<br>``` |
| Failure<br>Ex: If ID contains non-numeric values (invalid data)<br>Status Code – 404 Not Found | ```json<br>{<br>    "response": "DyWatchList@<watch_list_id>  was not<br>found",<br>    "status": "Failed"<br>``` |

| Response Status | Response |
|---|---|
| | `}` |
| Failure<br>Ex: If no match, Status Code – 200 | `{`<br>    `"response": "DyWatchList@<watch_list_id>  was not found",`<br>    `"status": "Failed"`<br>`}` |

## Get Watch List by Watch List Entry Value

This API retrieves watch lists which contains a watch list entry with given entry value.

**Release Added**: 6.3.0

**Input URL**      https://*<FortiSIEM_Supervisor_IP>*/phoenix/rest/watchlist/value

### Request Parameters

| Field | Type | Description |
|---|---|---|
| entryValue | String | Entry value of watch list entry. |

### Output

| Response Status | Response |
|---|---|
| Success | `{`<br>    `"response": [`<br>        `{`<br>            `"topGroup": true,`<br>            `"entries": [`<br>                `{`<br>                    `"lastSeen": null,`<br>                    `"naturalId": "172.30.57.65_1616469746578",`<br>                    `"dataCreationType": null,`<br>                    `"firstSeen": null,`<br>                    `"count": null,`<br>                    `"triggeringRules": null,`<br>                    `"description": "Testing",`<br>                    `"id": 888900,`<br>                    `"state": "Enabled",`<br>                    `"entryValue": "172.30.57.65",` |

| Response Status | Response |
|---|---|
| | <pre>                            "expiredTime": null,<br>                            "ageOut": "1w"<br>                    },<br>                    {<br>                            "lastSeen": null,<br>                            "naturalId": "PVVol_A001_A000356_POWER23_<br>1616480669538",<br>                            "dataCreationType": null,<br>                            "firstSeen": null,<br>                            "count": null,<br>                            "triggeringRules": "Datastore Space Warning",<br>                            "description": null,<br>                            "id": 889400,<br>                            "state": "Enabled",<br>                            "entryValue": "PVVol_A001_A000356_POWER23",<br>                            "expiredTime": null,<br>                            "ageOut": "1d"<br>                    }<br>                ],<br>                "isCaseSensitive": false,<br>                "dataCreationType": "USER",<br>                "displayName": "Test WL Group",<br>                "valueType": "STRING",<br>                "description": "",<br>                "id": 881750,<br>                "valuePattern": null,<br>                "ageOut": "1w"<br>            }<br>        ],<br>        "status": "Success"<br>}</pre> |
| Failure | <pre>{<br>        "response": "Reason for failure",<br>        "status": "Failed"<br>}</pre> |
| Failure<br>Ex: If no match,<br>Status Code – 200 | <pre>{<br>        "response":  "No such Watch List with entry value:  <entryValue><br>and watch list name: <watchlistName>",<br>        "status": "Failed"<br>}</pre> |

## Get Watch List by Watch List Entry ID

This API retrieves a specific watch list which contains a watch list entry with given entry ID.

**Release Added**: 6.3.0

**Input URL**    https://*<FortiSIEM_Supervisor_IP>*/phoenix/rest/watchlist/byEntry/*<watch_list_entry_id>*

## Request Path Parameters

| Field | Type | Description |
|---|---|---|
| Replace *<watch_list_entry_id>* with specific watch list entry id | Long | Watch list entry id |

## Output

| Response Status | Response |
|---|---|
| Success | ```{``` <br> ```    "response": {``` <br> ```        "topGroup": true,``` <br> ```        "entries": [``` <br> ```            {``` <br> ```                "lastSeen": null,``` <br> ```                "naturalId": "172.30.57.65_``` <br> ```1616469746578",``` <br> ```                "dataCreationType": null,``` <br> ```                "firstSeen": null,``` <br> ```                "count": null,``` <br> ```                "triggeringRules": null,``` <br> ```                "description": "Testing",``` <br> ```                "id": 888900,``` <br> ```                "state": "Enabled",``` <br> ```                "entryValue": "172.30.57.65",``` <br> ```                "expiredTime": null,``` <br> ```                "ageOut": "1w"``` <br> ```            },``` <br> ```            {``` <br> ```                "lastSeen": null,``` <br> ```                "naturalId": "PVVol_A001_A000356_POWER23_``` <br> ```1616480669538",``` <br> ```                "dataCreationType": null,``` <br> ```                "firstSeen": null,``` <br> ```                "count": null,``` <br> ```                "triggeringRules": "Datastore Space``` <br> ```Warning",``` <br> ```                "description": null,``` <br> ```                "id": 889400,``` <br> ```                "state": "Enabled",``` <br> ```                "entryValue": "PVVol_A001_A000356_``` <br> ```POWER23",``` <br> ```                "expiredTime": null,``` <br> ```                "ageOut": "1d"``` |

| Response Status | Response |
|---|---|
| | ```<br>                    }<br>                ],<br>                "isCaseSensitive": false,<br>                "dataCreationType": "USER",<br>                "displayName": "Test WL Group",<br>                "valueType": "STRING",<br>                "description": "",<br>                "id": 881750,<br>                "valuePattern": null,<br>                "ageOut": "1w"<br>        },<br>        "status": "Success"<br>}<br>``` |
| Failure<br>Ex: If ID contains non-numeric values (invalid data)<br>Status Code – 404 Not Found | ```<br>{<br>        "response": "Reason for failure",<br>        "status": "Failed"<br>}<br>``` |
| Failure<br>Ex: If no match, Status Code – 200 | ```<br>{<br>    "response": " No such watch list exists",<br>    "status": "Failed"<br>}<br>``` |

## Get Watch List Entry by Watch List Entry ID

This API retrieves a specific watch list entry given entry ID.

**Release Added**: 6.3.0

**Input URL**    https://*<FortiSIEM_Supervisor_IP>*/phoenix/rest/watchlist/entry/*<watch_list_entry_id>*

### Request Path Parameters

| Field | Type | Description |
|---|---|---|
| Replace *<watch_list_entry_id>* with specific watch list entry id. | Long | Watch list entry id |

### Output

| Response Status | Response |
|---|---|
| Success | { |

| Response Status | Response |
|---|---|
| | ```<br>    "response": {<br>        "lastSeen": null,<br>        "naturalId": "172.30.57.65_<br>1616469746578",<br>        "dataCreationType": null,<br>        "firstSeen": null,<br>        "count": null,<br>        "triggeringRules": null,<br>        "description": "Testing",<br>        "id": 888900,<br>        "state": "Enabled",<br>        "entryValue": "172.30.57.65",<br>        "expiredTime": null,<br>        "ageOut": "1w"<br>    },<br>    "status": "Success"<br>}<br>``` |
| Failure<br>Ex: If ID contains non-numeric values (invalid data)<br>Status Code – 404 Not Found | ```<br>{<br>        "response": "Reason for failure",<br>        "status": "Failed"<br>}<br>``` |
| Failure<br>Ex: If no match, Status Code – 200 | ```<br>{<br>"response": " No such watch list entry exists",<br>"status": "Failed"<br>}<br>``` |

# Update APIs

These POST APIs are available to update watch lists from the FortiSIEM database.

- Update State of Watch List Entry by Watch List Entry ID
- Update State of Watch List Entry by Watch List Entry Value
- Update Last Seen Time of Watch List Entry by Watch List Entry ID
- Update Last Seen Time of Watch List Entry by Watch List Entry Value
- Update Count of Watch List Entry by Watch List Entry ID
- Update Count of Watch List Entry by Watch List Entry Value
- Add Watch List Entry(s) to Watch List Groups
- Save Watch List Groups with Watch List Entry(s)
- Update Specific Watch List Entry

# Update State of Watch List Entry by Watch List Entry ID

This API allows user to update watch list entry state (i.e., make it active/inactive).

**Release Added**: 6.3.0

**Input URL**   https://*<FortiSIEM_Supervisor_IP>*/phoenix/rest/watchlist/entry/active/*<watch_list_entry_id>*

## Request Path Parameters

| Field | Type | Description |
|---|---|---|
| Replace *<watch_list _entry_id>* with specific watch list entry id | Long | Watch list entry id |

## Request Parameters

| Field | Type | Description |
|---|---|---|
| state | Boolean | Set specific entry to true/false state. |

## Output

| Response Status | Response |
|---|---|
| Success | ```{     "response": {         "lastSeen": null,         "naturalId": "172.30.57.65_1616469746578",         "dataCreationType": null,         "firstSeen": null,         "count": null,         "triggeringRules": null,         "description": "Testing",         "id": 888900,         "state": "Disabled",         "entryValue": "172.30.57.65",         "expiredTime": null,         "ageOut": "1w"     },     "status": "Success" }``` |
| Failure | ```{         "response": "Reason for failure",         "status": "Failed" }``` |
| Failure | ```{``` |

| Response Status | Response |
|---|---|
| Ex – If no match, status code - 200 | `            "response": "Can't update state of watch list entry - No such watch list entry exists",`<br>`            "status": "Failed"`<br>`}` |

# Update State of Watch List Entry by Watch List Entry Value

This API allows user to update the watch list entry state (i.e., make it active/inactive). This API requires a watch list group name where a required watch list entry exists.

**Release Added**: 6.3.0

**Input URL**　　　　https://*<FortiSIEM_Supervisor_IP>*/phoenix/rest/watchlist/entry/active

## Request Parameters

| Field | Type | Description |
|---|---|---|
| watchlistId | Long | Watchlist ID |
| value | String | Entry value of watch list entry |
| state | Boolean | Set specific entry to true/false state |
| custId | Long | Customer ID |

## Output

| Response Status | Response |
|---|---|
| Success | `{`<br>`    "response": {`<br>`        "lastSeen": null,`<br>`        "naturalId": "PVVol_A001_A000356_POWER23_1616480669538",`<br>`        "dataCreationType": null,`<br>`        "firstSeen": null,`<br>`        "count": 10,`<br>`        "triggeringRules": "Datastore Space Warning",`<br>`        "description": null,`<br>`        "id": 889400,`<br>`        "state": "Disabled",`<br>`        "entryValue": "PVVol_A001_A000356_POWER23",`<br>`        "expiredTime": null,`<br>`        "ageOut": "1d"`<br>`    },` |

| Response Status | Response |
|---|---|
|  | ```"status": "Success"```<br><br>```}``` |
| Failure | ```{```<br><br>```        "response": "Reason for failure",```<br>```        "status": "Failed"```<br><br>```}``` |
| Failure<br>Ex – If no match, status code - 200 | ```{```<br><br>```        "response": "Can't update state of watch list entry - No such```<br>```watch list entry exists",```<br>```        "status": "Failed"```<br><br>```}``` |

# Update Last Seen Time of Watch List Entry by Watch List Entry ID

This API allows user to update watch list entry's last seen time.

**Release Added**: 6.3.0

**Input URL**   https://<*FortiSIEM_Supervisor_IP*>/phoenix/rest/watchlist/entry/lastseen/<*watch_list_entry_id*>

## Request Path Parameters

| Field | Type | Description |
|---|---|---|
| Replace <*watch_list_ entry _id*> with specific watch list entry id | Long | Watch list entry id |

## Request Parameters

| Field | Type | Description |
|---|---|---|
| lastSeenTime | Long | Long value of last seen time i.e. Unix timestamp |
| custId | Long | Customer ID |

## Output

| Response Status | Response |
|---|---|
| Success | ```{```<br><br>```        "response": {``` |

| Response Status | Response |
|---|---|
|  | ```json
        "lastSeen": 1612901760000,
        "naturalId": "PVVol_A001_A000356_POWER23_1616480669538",
        "dataCreationType": null,
        "firstSeen": null,
        "count": 10,
        "triggeringRules": "Datastore Space Warning",
        "description": null,
        "id": 889400,
        "state": "Disabled",
        "entryValue": "PVVol_A001_A000356_POWER23",
        "expiredTime": 1612988160000,
        "ageOut": "1d"
    },
    "status": "Success"
}
``` |
| Failure<br>Ex: If ID contains non-numeric values (invalid data)<br>Status Code – 404 Not Found | ```json
{
        "response": "Reason for failure",
        "status": "Failed"
}
``` |
| Failure<br>Ex – If no match, status code - 200 | ```json
{
        "response": "Can't update last seen time of watch list
entry - No such watch list entry exists",
        "status": "Failed"
}
``` |

## Update Last Seen Time of Watch List Entry by Watch List Entry Value

This API allows the user to update watch list entry's last seen time. This API requires a watch list group name where the required watch list entry exists.

**Release Added**: 6.3.0

| Input URL | https://*<FortiSIEM_Supervisor_IP>*/phoenix/rest/watchlist/entry/lastseen |
|---|---|

### Request Parameters

| Field | Type | Description |
|---|---|---|
| watchlistId | Long | Watchlist ID |
| value | String | Entry value of watch list entry |
| lastSeenTime | Long | Long value of last seen time i.e. Unix timestamp |
| custId | Long | Customer ID |

## Output

| Response Status | Response |
|---|---|
| Success | ```<br>{<br>    "response": {<br>        "lastSeen": 1612901760001,<br>        "naturalId": "PVVol_A001_A000356_POWER23_1616480669538",<br>        "dataCreationType": null,<br>        "firstSeen": null,<br>        "count": 10,<br>        "triggeringRules": "Datastore Space Warning",<br>        "description": null,<br>        "id": 889400,<br>        "state": "Disabled",<br>        "entryValue": "PVVol_A001_A000356_POWER23",<br>        "expiredTime": 1612988160001,<br>        "ageOut": "1d"<br>    },<br>    "status": "Success"<br>}<br>``` |
| Failure | ```<br>{<br>        "response": "Reason for failure",<br>        "status": "Failed"<br>}<br>``` |
| Failure<br><br>Ex – If no match, status code - 200 | ```<br>{<br>        "response": "Can't update last seen time of watch list entry - No such watch list entry exists",<br>        "status": "Failed"<br>}<br>``` |

## Update Count of Watch List Entry by Watch List Entry ID

This API allows user to update watch list entry's count.

**Release Added**: 6.3.0

**Input URL**    https://<*FortiSIEM_Supervisor_IP*>/phoenix/rest/watchlist/entry/count/<*watch_list_entry_id*>

## Request Path Parameters

| Field | Type | Description |
|---|---|---|
| Replace <*watch_list_ entry _id*> with specific watch list entry id | Long | Watch list entry id |

## Request Parameters

| Field | Type | Description |
|---|---|---|
| count | Long | Count of watch list entry occurrence |

## Output

| Response Status | Response |
|---|---|
| Success | ```<br>{<br>    "response": {<br>        "lastSeen": 1612901760001,<br>        "naturalId": "PVVol_A001_A000356_POWER23_<br>1616480669538",<br>        "dataCreationType": null,<br>        "firstSeen": null,<br>        "count": 100,<br>        "triggeringRules": "Datastore Space Warning",<br>        "description": null,<br>        "id": 889400,<br>        "state": "Disabled",<br>        "entryValue": "PVVol_A001_A000356_POWER23",<br>        "expiredTime": 1612988160001,<br>        "ageOut": "1d"<br>    },<br>    "status": "Success"<br>}<br>``` |
| Failure<br>Ex: If ID contains non-numeric values (invalid data)<br>Status Code – 404 Not Found | ```<br>{<br>        "response": "Reason for failure",<br>        "status": "Failed"<br>}<br>``` |
| Failure<br>Ex – If no match, status code - 200 | ```<br>{<br>        "response": "Can't update count of watch list entry - No<br>such watch list entry exists",<br>        "status": "Failed"<br>}<br>``` |

## Update Count of Watch List Entry by Watch List Entry Value

This API allows user to update watch list entry's count. This API requires watch list group name where required watch list entry exists.

**Release Added**: 6.3.0

**Input URL**     https://<*FortiSIEM_Supervisor_IP*>/phoenix/rest/watchlist/entry/count

## Request Parameters

| Field | Type | Description |
|-------|------|-------------|
| custId | Long | Customer ID |
| watchlistId | Long | Watchlist ID |
| value | String | Entry value of watch list entry |
| count | Long | Count of watch list entry occurrence |

## Output

| Response Status | Response |
|-----------------|----------|
| Success | ```<br>{<br>    "response": {<br>        "lastSeen": 1612901760001,<br>        "naturalId": "PVVol_A001_A000356_POWER23_1616480669538",<br>        "dataCreationType": null,<br>        "firstSeen": null,<br>        "count": 100,<br>        "triggeringRules": "Datastore Space Warning",<br>        "description": null,<br>        "id": 889400,<br>        "state": "Disabled",<br>        "entryValue": "PVVol_A001_A000356_POWER23",<br>        "expiredTime": 1612988160001,<br>        "ageOut": "1d"<br>    },<br>    "status": "Success"<br>}<br>``` |
| Failure | ```<br>{<br>        "response": "Reason for failure",<br>        "status": "Failed"<br>}<br>``` |
| Failure<br>Ex – If no match, status code - 200 | ```<br>{<br>        "response": "Can't update count of watch list entry - No such watch list entry exists",<br>        "status": "Failed"<br>}<br>``` |

# Add Watch List Entry(s) to Watch List Groups

This API allows user to add watch list entry(s) to one or more watch list groups.

**Release Added**: 6.3.0

**Input URL**     https://<*FortiSIEM_Supervisor_IP*>/phoenix/rest/watchlist/addTo

## Request Parameters

| Field | Type | Description |
|---|---|---|
| watchlistId | Long | Watchlist ID |

## Request Body

| Field | Type | Description |
|---|---|---|
| Body | JSON Array of Watch list entry objects | Watch Entry |
| | | |
| **entryValue(required)** | String | Watch List entry value |

```
[
                {
                    "inclusive": false,
                    "count": 10,
                    "custId": 1,
                    "triggeringRules": "Datastore Space Warning",
                    "entryValue": "PVVol_A001_A000356_POWER2",
                    "ageOut": "1d",
                    "lastSeen": 1613601369215,
                    "firstSeen": 1613601369215,
                    "disableAgeout": false,
                    "dataCreationType": "USER"
                }
]
```

## Output

| Response Status | Response |
|---|---|
| Success | ```{     "response": "Successfully added to watch list - [IDs]",     "status": "Success" }``` |
| Failure | ```{         "response": "Reason for failure",         "status": "Failed"``` |

| Response Status | Response |
|---|---|
| | `}` |
| Failure<br><br>Ex: Invalid data format in request parameters<br><br>Status code - 200 | `{`<br>`    "response": " Error while adding entries to watch lists -`<br>`Invalid data format",`<br>`    "status": "Failed"`<br>`}` |
| Failure<br><br>Ex: If no entry value exists in Watchlist Entry<br><br>Status code - 200 | `{`<br>`    "response": "Error while adding entries to watch lists -`<br>`WatchListEntry must have entryValue field",`<br>`    "status": "Failed"`<br>`}` |

# Save Watch List Groups with Watch List Entry(s)

This API allows user to save one or more watch list groups to FSM database. Each watch list can contain one or more watch list entries.

**Release Added**: 6.3.0

| Input URL | https://<*FortiSIEM_Supervisor_IP*>/phoenix/rest/watchlist/save |
|---|---|

## Request Body

| Field | Type | Description |
|---|---|---|
| Body | JSON Object of Watch list with watch list entry | Watch list with entry(s) |
| | | |
| displayName (required) | String | Display name for watch list group |
| type (required) | String | Group type - ENUM |
| entryValue (required) | String | Entry value of DyWatchlistEntry |
| dataCreationType | String | Enum – {SYSTEM, USER}<br><br>If value is null – Default value will be 'SYSTEM' |
| | | |
| `{`<br><br>`            "description": "Servers, network or storage devices",` | | |

| Field | Type | Description |
|---|---|---|
| | | ```
"displayName": "Resource Issues Test4",
"type": "DyWatchList",
"isCaseSensitive": false,
"dataCreationType": "USER",
"topGroup": false,
"valuePattern": null,
"valueType": "STRING",
"ageOut": "1d",
"custId": 1,
"entries": [{
        "inclusive": true,
        "entryValue": "PVVol_A001_A000356_5new",
        "ageOut": "1d",
        "count": 1,
        "custId": 1,
        "firstSeen": 1612901760000,
        "lastSeen": 1612901760000,
        "triggeringRules": "Datastore Space
Warning",
        "dataCreationType": "USER"
}]
}
``` |

## Output

| Response Status | Response |
|---|---|
| Success | ```
{
    "response": [
        {
            "topGroup": false,
            "entries": [
                {
                    "lastSeen": 1612901760000,
                    "naturalId": "Nid",
                    "dataCreationType": "USER",
                    "firstSeen": 1612901760000,
                    "count": 1,
                    "triggeringRules": "Datastore
Space Warning",
                    "description": null,
                    "id": 0,
                    "state": "Enabled",
                    "entryValue": null,
                    "expiredTime": null,
                    "ageOut": "1d"
``` |

| Response Status | Response |
|---|---|
| | ```<br>                }<br>            ],<br>            "isCaseSensitive": null,<br>            "dataCreationType": "SYSTEM",<br>            "displayName": "Resource Issues Test WL<br>Grp4",<br>            "valueType": "STRING",<br>            "description": "Servers, network or<br>storage devices",<br>            "id": 899753,<br>            "valuePattern": null,<br>            "ageOut": null<br>        }<br>    ],<br>    "status": "Success"<br>}<br>``` |
| Failure | ```<br>{<br>        "response": "Reason for failure",<br>        "status": "Failed"<br>}<br>``` |
| Failure<br>Ex: If entry doesn't have entry value<br>Response code - 200 | ```<br>{<br>   "response" : "Error while saving watch lists -<br>WatchListEntry must have entryValue field",<br>   "status" : "Failed"<br>}<br>``` |
| Failure<br>Ex:<br>• If display name is duplicate (already exists) or body doesn't have filed – 'type'<br>• Unrecognized fields in POST body<br>Response code - 200 | ```<br>{<br>    "response": "Failed to save watchlist",<br>    "status": "Failed"<br>}<br>``` |

# Update Specific Watch List Entry

This API allows user to update any watch list entry. The JSON object of watch list entry must contain valid watch list entry id otherwise it will be saved as a new entry to ungrouped watch list.

**Release Added**: 6.3.0

**Input URL**      https://*<FortiSIEM_Supervisor_IP>*/phoenix/rest/watchlist/entry/save

## Request Body

| Field | Type | Description |
|---|---|---|
| Body | JSON Object of Watch list with watch list entry | Watch list entry |
| | | |
| **entryValue(required)** | String | Watch list entry value |
| | | |

```
{
    "lastSeen": 1612901760002,
    "dataCreationType": "USER",
    "firstSeen": 1612901760001,
    "count": 100,
    "custId": 1
    "triggeringRules": "Datastore Space Warning",
    "description": "Testing again",
    "id": 889400,
    "inclusive": true,
    "entryValue": "PVVol_A001_A000356_POWER23",
    "expiredTime": 1612988160001,
    "ageOut": "2d",
}
```

**Note**: ID is mandatory to update watch list entry. If there is no id in JSON body, a new entry will be created.

## Output

| Response Status | Response |
|---|---|
| Success | ```
{
    "response": {
        "lastSeen": 1612901760002,
        "naturalId": "PVVol_A001_A000356_POWER23_
1612901760002",
        "dataCreationType": "USER",
        "firstSeen": 1612901760001,
        "count": 100,
        "triggeringRules": "Datastore Space Warning",
        "description": "Testing again",
        "id": 889400,
        "state": "Enabled",
        "entryValue": "PVVol_A001_A000356_POWER23",
        "expiredTime": 1613074560002,
        "ageOut": "2d"
    },
    "status": "Success"
``` |

| Response Status | Response |
|---|---|
| | ``` } ``` |
| Failure | ```{           "response": "Reason for failure",           "status": "Failed"   } ``` |
| Failure<br>Ex: If entry doesn't have entry value<br>Response code - 200 | ```{     "response": "HTTP 400 Bad Request",     "status": "Failed"   } ``` |

# Delete APIs

The following **POST** Delete APIs are available.

- Delete Watch List Entry by ID
- Delete Watch List by ID

## Delete Watch List Entry by ID

This API allows user to delete watch list entry(s).

**Release Added**: 6.3.0

| Input URL | https://*<FortiSIEM_Supervisor_IP>*/phoenix/rest/watchlist/entry/delete |
|---|---|

### Request Body

| Field | Type | Description |
|---|---|---|
| | List of Long values | Watch List Entry ids |
| Ex: [500000, 500001] | | |

### Output

| Response Status | Response |
|---|---|
| Success | ```{           "response": "Deleted entries - [IDs]", ``` |

| Response Status | Response |
|---|---|
| | `        "status": "Success"`<br>`}` |
| Failure | `{`<br>`        "response": "Reason for failure",`<br>`        "status": "Failed"`<br>`}` |
| Failure<br>Ex: If any exception occurs | `{`<br>`            "response": " Error in deleting watch list entries -`<br>`Exception message ",`<br>`        "status": "Failed"`<br>`}` |

# Delete Watch List by ID

This API allows user to delete watch list(s).

**Release Added**: 6.3.0

**Input URL**        https://<*FortiSIEM_Supervisor_IP*>/phoenix/rest/watchlist/delete

## Request Body

| Field | Type | Description |
|---|---|---|
| | List of Long values | Watch list ids |
| Ex: [500000, 500001] | | |

## Output

| Response Status | Response |
|---|---|
| Success | `{`<br>`            "response": "Deleted watch lists - [IDs]",`<br>`        "status": "Success"`<br>`}` |
| Failure | `{`<br>`        "response": "Reason for failure",`<br>`        "status": "Failed"`<br>`}` |
| Failure | `{`<br>`            "response": "Deleting system defined group is` |

| Response Status | Response |
|---|---|
| Ex: If group is system defined group | ```<br>not allowed",<br>          "status": "Failed"<br>}<br>``` |
| Failure<br>Ex: If any exception occurs | ```<br>{<br>                  "response": " Error in deleting watch lists –<br>Exception message ",<br>          "status": "Failed"<br>}<br>``` |

# JSON Object Formats

- Watch List Entry JSON
- Watch List JSON

## Watch List Entry JSON

| Field | Type | Description |
|---|---|---|
| id | Long | Watch list entry id |
| firstSeen | Long | First seen time – Unix format |
| lastSeen | Long | Last seen time – Unix format |
| expiredTime | Long | Expiry time – Unix format |
| state | String | State of entry – Enabled/Disabled |
| naturalId | String | Unique ID of watch list entry |
| triggeringRules | String | FSM Rules – Comma separated |
| entryValue | String | Entry value of Watch list entry |
| description | String | Description |
| ageOut | String | Age out (Expiry) |
| count | Long | Occurrence count |
| dataCreationType | ENUM | [SYSTEM, USER] |

# Watch List JSON

| Field | Type | Description |
|---|---|---|
| id | Long | Watch list group id |
| naturalId | String | Unique ID of watch list |
| isCaseSensitive | Boolean | |
| ageOut | String | Age out (Expiry) |
| entries | List<WatchListEntry> | List of Entries Refer to Watch List Entry JSON Table. |
| displayName | String | Display name of watch list group |
| name | String | Name of the watch list |
| description | String | Entry value of Watch list description |
| valueType | ENUM | Value type - STRING, IP, etc... |
| topGroup | Boolean | True/false |
| dataCreationType | ENUM | [SYSTEM, USER] |
| valuePattern | ENUM | [IP, IPRANGE, CIDR] |

# Example Usage

The sample codes provided are for instructional use only. Please adapt it to your environment. Download the appropriate zip file containing the samples from the following URLs:

## Example Performance and Health, CMDB Device, and Event/Query Worker Configuration APIs

A zip file containing example Performance and Health, CMDB Device (APIs 6-12), and Event/Query Worker Configuration API files is available here.

## Python Support

### Python 2.7 Release

https://filestore.fortinet.com/docs.fortinet.com/upload/fsiem_rest_api_630.zip

2.7 scripts are tested using version 2.7.16. You must install `httplib2` and ssl manually, if they are not already installed.

### Python 3.9 Release

https://help.fortinet.com/fsiem/Public_Resource_Access/rest_api_python3/fsiem_rest_api_python3.zip

3.9 scripts are tested using version 3.9.0. You must install `httplib2` and ssl manually, if they are not already installed.

# Appendix

- Description of Device Attributes
- Description of Health JSON Attributes
- Current Thresholds for Health Status

## Description of Device Attributes

The following tables are available for device attributes.

- Device Attribute
- Bios
- Patch
- Processor
- Storage
- Network Interface
- Installed Software
- Running Software/Application
- swService
- Monitor Types
- Event Pulling Types
- Error Messages

| Device Attribute | Type | Description |
|---|---|---|
| unmanaged | boolean | Identifies if the device is managed or unmanaged. |
| discoverMethod | string | The discovery method of the device. |
| accessMethodIds | string | The ids for the access method. |
| discoverTime | unsignedLong | The date and time the device was discovered. |
| name | string | The device name. |
| accessIP | string | The IP address. |
| vendor | string | The vendor name. |
| model | string | The model name. |
| version | string | The version. |
| buildNumber | string | The build number. |
| osSerialNum | string | The operating system's serial number. |

| Device Attribute | Type | Description |
|---|---|---|
| osEdition | string | The edition of the operating system. |
| hwVendor | string | The hardware vendor. |
| assetCategory | string | The category that the asset belongs to. |
| assetWeight | unsignedByte | The weight (priority) given to the asset. |
| description | string | Any additional details/information. |
| sysUptime | unsignedInt | The system uptime. |
| bios | | See bios table. |

| bios | Type | Description |
|---|---|---|
| name | string | The bios name. |
| vendor | string | The vendor from where the bios came from. |
| serialNumber | string | The bios serial number. |
| version | string | The bios version. |

| Patch | Type | Description |
|---|---|---|
| Name | string | The name of the patch. |
| Description | string | Information about the patch. |
| installedBy | string | The person who installed the patch. |
| installedOn | unsignedInt | The date and time the patch was installed. |

| Processor | Type | Description |
|---|---|---|
| name | string | The processor name. |
| cpuUtil | unsignedByte | The CPU utilization of the processor. |
| manufacturer | string | The name of the processor manufacturer. |
| addrWidth | unsignedByte | The width of the DMA address space (in bytes). |
| dataWidth | unsignedByte | The maximum space available for data (in bytes) |
| currClockSpeed | unsignedShort | The current clock speed of the processor. |
| maxClockSpeed | unsignedShort | The maximum clock speed of the processor. |

| Storage | Type | Description |
|---|---|---|
| type | string | The storage type. |
| description | string | Information about the storage. |
| size | string | The storage size. |
| used | string | The amount of storage used. |
| memUtil | unsignedByte | The amount of storage utilized for memory. |
| diskUtil | unsignedByte | The amount of disk utilization from storage. |

| networkInterface | Type | Description |
|---|---|---|
| type | string | The network interface type. |
| name | string | Name of the network interface. |
| alias | string | The network alias name. |
| description | string | Information/details about the network interface. |
| ipv4Addr | string | The IPv4 address. |
| ipv4Mask | unsignedByte | The IPv4 subnet mask. |
| macAddr | string | The media access control address (MAC address). |
| speed | string | The Ethernet transmission speed. |
| snmpIndex | unsignedByte | The unique value of the interface. |
| isTrunk | boolean | Whether the network interface uses trunking or not. |
| adminStatus | string | The configured status of the interface (port). |
| operStatus | string | The working/running status of the interface. |

| InstalledSoftware | Type | Description |
|---|---|---|
| custId | unsignedByte | The customer id. |
| count | unsignedByte | The number of installed software. |

| runningSoftware | Type | Description |
|---|---|---|
| name | string | The name of the application. |
| groupName | string | The name of the application group that the application belongs to. |
| processName | string | The application's process name. |

| runningSoftware | Type | Description |
|---|---|---|
| param | string | The application parameters. |
| procOwner | | The process owner of the application. |
| path | string | The location of the application. |
| uptime | unsignedInt | The uptime of the running application. |

| swService | Type | Description |
|---|---|---|
| name | string | The service name. |
| displayName | string | The display name of the service. |
| description | string | Description of the service. |
| processId | unsignedShort | The service process Id. |
| path | string | The location of the service. |
| state | string | The current service state. |
| status | string | The status of the service. |
| startMode | string | The start up mode of the service. |

| monitorTypes | Type | Description |
|---|---|---|
| refId | unsignedInt | The reference Id. |

| eventPullingTypes | Type | Description |
|---|---|---|
| id | string | The id of the pulling event type. |

| errorMsgs | Type | Description |
|---|---|---|
| accessMethod | string | The access method error message. |
| error | string | The error message. |
| severity | string | The severity of the error. |
| impact | string | The impact of the error. |
| resolution | string | The resolution required to fix the error. |

# Description of Health JSON Attributes

The following table provides a description of health attributes for FortiSIEM Manager, Supervisor, Worker, and Collector.

| JSON Node | Attribute | Applicability | Description |
|---|---|---|---|
| instances | id | All | Instance Id |
| instances | name | All | Instance name |
| instances | healthStatus | All | Instance health based on Supervisor and Worker health: Normal/Warning/Critical. Collector health is now ignored. |
| nodes.summary.instanceId | instanceId | All | Instance Id as it appears in FortiSIEM Manager. This is defined when an Instance registers to the Manager. |
| nodes.summary.name | name | All | Name as it appears in the Supervisor GUI. |
| nodes.summary.nodeType | nodeType | All | Manager/Supervisor/Worker/Collector |
| nodes.summary.status | status | All | Health of the node: Normal/Warning/Critical |
| nodes.metrics.healthSummary | summary | All | Health of the node - Normal/Warning/Critical |
| nodes.metrics.healthSummary.reason | attribute | All | Name of attribute e.g. CPU Utilization etc. See Appendix - Current Thresholds for Health Status for a complete list. |
| nodes.metrics.healthSummary.reason | value | All | Normal/Warning/Critical |
| nodes.metrics.healthSummary.reason | reason | All | Reason explaining the value |
| nodes.metrics | lastUpdateTime | Worker | Last time a health update was received from this node. |
| nodes.metrics | lastFileRecvTime | Worker | Last time a file was received from Collector (Unix epoch time). |
| nodes.metrics | lastEventTime | Worker | Last time a heartbeat was received from Collector (Unix epoch time). |
| nodes.metrics.hostInfo | name | All | Host Name (same as nodes.summary.name) |
| nodes.metrics.hostInfo | ip | All | Host IP |

| JSON Node | Attribute | Applicability | Description |
| --- | --- | --- | --- |
| nodes.metrics.versionInfo | version | All | FortiSIEM Image Version |
| nodes.metrics.versionInfo | commitHash | All | FortiSIEM Image Commit hash (SHA-1 hash made up of a few properties from the code commit.) |
| nodes.metrics.versionInfo | builtOn | All | Day when the image was built (Unix Epoch time). |
| nodes.metrics.versionInfo | contentVersion | All | FortiSIEM Content version running on this node. |
| nodes.metrics.hardware | vCPU | All | Number of vCPUs in this node |
| nodes.metrics.hardware | memory_gb | All | Total physical memory in this node |
| nodes.metrics.eps | 3min | All | Average EPS calculated at 3 minute intervals. |
| nodes.metrics.eps | 15min | All | Average EPS calculated at 15 minute intervals. |
| nodes.metrics.eps | 30min | All | Average EPS calculated at 30 minute intervals. |
| nodes.metrics.eps | allocatedEPS | All | EPS allocated to a node (limited by license). |
| nodes.metrics.eps | incomingEPS | All | Incoming EPS to this node |
| nodes.metrics.eps | dropLicenseEPS | All | Dropped EPS because of license |
| nodes.metrics.eventUploadQueue | queue | Worker | Number of files in Event Upload Queue at Worker - this queue stores filed uploaded by Collector. |
| nodes.metrics.eventUploadQueue | disk_kb | Worker | Total file size in Event Upload Queue at Worker - this queue stores filed uploaded by Collector. |
| nodes.metrics.eventUploadQueue | total_mb | Collector | Total file size in Collector waiting to be uploaded to Worker or Supervisor. |
| nodes.metrics.eventUploadQueue | event_mb | Collector | Total event file size in Collector waiting to be uploaded to Worker or Supervisor. |
| nodes.metrics.eventUploadQueue | windows_mb | Collector | Total Windows Agent file size in Collector waiting to be uploaded to Worker or Supervisor. |
| nodes.metrics.eventUploadQueue | linux_mb | Collector | Total Linux Agent file size in Collector waiting to be uploaded to Worker or Supervisor. |

| JSON Node | Attribute | Applicability | Description |
|-----------|-----------|---------------|-------------|
| nodes.metrics.eventUploadQueue | svn_mb | Collector | Total Configuration (SVNLite) file size in Collector waiting to be uploaded to Worker or Supervisor. |
| nodes.metrics.loadAverage | 1min | All | 1 minute load average |
| nodes.metrics.loadAverage | 5min | All | 5 minute load average |
| nodes.metrics.loadAverage | 15min | All | 15 minute load average |
| nodes.metrics.cpuUsage | used_pct | All | Total CPU Utilization |
| nodes.metrics.cpuUsage | system_pct | All | System CPU utilization |
| nodes.metrics.cpuUsage | user_pct | All | User CPU Utilization |
| nodes.metrics.cpuUsage | free_pct | All | Free CPU Utilization |
| nodes.metrics.cpuUsage | idleWait_pct | All | Percentage of time CPU is waiting for I/O to complete. |
| nodes.metrics.memoryUsage | total_mb | All | Total Memory (MB) |
| nodes.metrics.memoryUsage | used_mb | All | Used Memory (MB) |
| nodes.metrics.memoryUsage | free_mb | All | Free Memory (MB) |
| nodes.metrics.memoryUsage | used_pct | All | Memory Utilization (pct) |
| nodes.metrics.swapUsage | total_mb | All | Total Swap memory (MB) |
| nodes.metrics.swapUsage | used_mb | All | Used Swap Memory (MB) |
| nodes.metrics.swapUsage | in_bps | All | Swap In rate (Bits/sec) |
| nodes.metrics.swapUsage | out_bps | All | Swap Out rate (Bits/sec) |
| nodes.metrics.swapUsage | used_pct | All | Swap Utilization |
| nodes.metrics.diskUsage | filesystem | All | File system |
| nodes.metrics.diskUsage | mountedOn | All | File system mount point like /svn, /cmdb etc |
| nodes.metrics.diskUsage | type | All | File system type e.g. xfs |
| nodes.metrics.diskUsage | size_mb | All | Total File system Size (MB) |
| nodes.metrics.diskUsage | used_mb | All | Used File system Size (MB) |
| nodes.metrics.diskUsage | avail_mb | All | Free File system Size (MB) |
| nodes.metrics.diskUsage | used_pct | All | Percentage of file system used. |
| nodes.metrics.upgradeStat | upgradeVersion | Collector | Last Image version the Collector upgraded to. |

| JSON Node | Attribute | Applicability | Description |
|---|---|---|---|
| nodes.metrics.upgradeStat | installStatus | Collector | Last Image version install status (Completed or Failed followed by reason.) |
| nodes.metrics.upgradeStat | downloadStatus | Collector | Last Image version download status (Completed or Failed followed by reason.) |
| nodes.metrics.diskIO | device | All | Linux device for measuring disk I/O |
| nodes.metrics.diskIO | mountedOn | All | Device mount point like /svn, /cmdb etc |
| nodes.metrics.diskIO | read_ops | All | Read Operations/sec |
| nodes.metrics.diskIO | write_ops | All | Write Operations/sec |
| nodes.metrics.diskIO | read_kbps | All | Read Volume (KB/sec) |
| nodes.metrics.diskIO | write_kbps | All | Write Volume (KB/sec) |
| nodes.metrics.diskIO | readWait_ms | All | Read Wait Latency (msec) |
| nodes.metrics.diskIO | writeWait_ms | All | Write Wait Latency (msec) |
| nodes.metrics.diskIO | util_pct | All | Disk I/O utilization |
| nodes.metrics.nfsIO | location | Super, Worker | Remote path |
| nodes.metrics.nfsIO | path | Super, Worker | Local directory (e.g. /data) |
| nodes.metrics.nfsIO | read_ops | Super, Worker | NFS Read Operations/second for EventDB based deployments |
| nodes.metrics.nfsIO | read_kbps | Super, Worker | NFS Read Volume (KBytes/second) for EventDB based deployments |
| nodes.metrics.nfsIO | read_kbpop | Super, Worker | NFS Read Volume (Kbytes/operation) for EventDB based deployments |
| nodes.metrics.nfsIO | readLatency_ms | Super, Worker | NFS Read Latency (ms) for EventDB based deployments |
| nodes.metrics.nfsIO | write_ops | Super, Worker | NFS WriteOperations/second for EventDB based deployments |
| nodes.metrics.nfsIO | write_kbps | Super, Worker | NFS WriteVolume (KBytes/second) for EventDB based deployments |
| nodes.metrics.nfsIO | write_kbpop | Super, Worker | NFS Write Volume (Kbytes/operation) for EventDB based deployments |
| nodes.metrics.nfsIO | writLatency_ms | Super, Worker | NFS Write Latency (ms) for EventDB based deployments |

| JSON Node | Attribute | Applicability | Description |
|---|---|---|---|
| nodes.metrics.processStat | processName | All | FortiSIEM process name |
| nodes.metrics.processStat | owner | All | FortiSIEM process owner |
| nodes.metrics.processStat | uptime_sec | All | Process Uptime (seconds) |
| nodes.metrics.processStat | cpuUtil_pct | All | Process CPU Utilization |
| nodes.metrics.processStat | residentMemory_mb | All | Process Resident Memory Usage (MB) |
| nodes.metrics.processStat | memoryUtil_pct | All | Process Memory Utilization |
| nodes.metrics.processStat | diskRead_kbps | All | Process Aggregate Disk Read Volume (KB/sec) |
| nodes.metrics.processStat | diskWrite_kbps | All | Process Aggregate Write Volume (KB/sec) |
| nodes.metrics.processStat | sharedStore_type | All | Reader or Writer or none |
| nodes.metrics.processStat | sharedStore_position | All | Shared store read/write position (Bytes written or read.) |
| nodes.metrics.processStat | sharedStore_pct | All | Shared store read/write position (Percentage) - 100% means end of circular buffer. |

# Current Thresholds for Health Status

The following table provides information on what normal thresholds are for certain Health JSON attributes.

| Health JSON Attribute | Applicability | Threshold |
|---|---|---|
| CPU Utilization | All nodes | • Normal - if cpuUsage.used_pct less than 75 AND loadAverage 15 minutes less than nodes.hardware.vCPU and the loadAverage of last 15 minutes are less than 1 * number_of_cores<br>• Warning - if (cpuUsage.used_pct between (75 and 90) OR (loadAverage 15 minutes between (nodes.hardware.vCPU and 2* nodes.hardware.vCPU) and the loadAverage of the last 15 minutes are less than 2 * number_of_cores<br>• if cpuUsage.used_pct greater than 90 OR loadAverage 15 minutes greater than 2*nodes.hardware.vCPU and the loadAverage of the last 15 minutes is greater than 2 * number_of_cores |
| Memory Utilization | All nodes | • Normal - if memoryUsage.used_pct less than 75<br>• Warning - if memoryUsage.used_pct between 75 and 90<br>• Critical - if memoryUsage.used_pct greater than 90 |

| Health JSON Attribute | Applicability | Threshold |
|---|---|---|
| Swap Space Utilization | All nodes | • Normal - if swapUsage.in_bps less than 7Mbps<br>• Warning - if swapUsage.in_bps between 7Mbps and 10Mbps<br>• Critical - if swapUsage.in_bps greater than 10Mbps |
| Disk Utilization | All nodes; skips /data, data-clickhouse | • Normal - if diskUsage.used_pct less than 65<br>• Warning - if diskUsage.used_pct between 65 and 85<br>• Critical - if diskUsage.used_pct greater than 85 |
| I/O Utilization | All nodes | • Normal - if cpuUsage.ioWait_pct less than 15 AND diskIO.readWait_ms less than 30 AND diskIO.writeWait_ms less than 30 AND nfsIO.readLatency_ms less than 50 AND nfsIO.writeLatency_ms less than 50<br>• Warning - if cpuUsage.ioWait_pct between (15 and 30) OR diskIO.readWait_ms between (30 and 60) OR diskIO.writeWait_ms between (30 and 60) AND nfsIO.readLatency_ms between (50 and 75) AND nfsIO.writeLatency_ms between 50 and 75<br>• Critical - if cpuUsage.ioWait_pct more than 30 OR diskIO.readWait_ms more than 60 OR diskIO.writeWait_ms more than 60 OR nfsIO.readLatency_ms more than 75 OR nfsIO.writeLatency_ms more than 75 |
| Process Health | All nodes | • Normal - if processStat.uptime more than 1 hour AND processStat.cpuUtil_pct less than 50 AND processStat.memoryUtil_pct less than 50<br>• Warning - if processStat.uptime less than 1 hour OR processStat.cpuUtil_pct between (50 and 75) OR processStat.memoryUtil_pct between (50 and 75)<br>• Critical - if process is DOWN OR processStat.cpuUtil_pct greater than 75 OR processStat.memoryUtil_pct greater than 75 |
| Event Pipeline | Collector only | This indicates whether queues are building up in Collectors.<br>• Normal - if eventUploadQueue.total_mb less than 20<br>• Warning - if eventUploadQueue.total_mb between 20 and 50<br>• Critical - if eventUploadQueue.total_mb greater than 50 |
| Event Pipeline | Worker only | This indicates whether queues are building up in Workers and may be caused by Workers slow in ingesting events to storage.<br>• Normal - if eventUploadQueue.disk_mb less than 25<br>• Warning - if eventUploadQueue.disk_mb between 25 and 75<br>• Critical - if eventUploadQueue.disk_mb greater than 75 |
| Shared Store | Worker, Supervisor | This indicates that some FortiSIEM processes are slow in processing events and may eventually block the writer phParser process from ingesting events. Events may eventually be lost.<br>• Normal - if difference between reader and writer's sharedStore_pct is less than 15 |

| Health JSON Attribute | Applicability | Threshold |
|---|---|---|
| | | • Warning - if difference between reader and writer's sharedStore_pct is between 15 and 30<br>• Critical - if difference between reader and writer's sharedStore_pct is more than 30 |
| Last Status Updated | All nodes | This is based on the health updates between Collector and Supervisor; Worker and Supervisor; and Instance Supervisor and FortiSIEM Manager.<br>• Normal - if nodes.metrics.lastStatusUpdated less than 15 minute delay<br>• Warning - if nodes.metrics.lastStatusUpdated between (15 minute and 20 minute) delay<br>• Critical - if nodes.metrics.lastStatusUpdated more than 20 minute delay |
| Last Event Time | Collector | This information is sent by each Worker to Supervisor based on what each Worker receives from Collectors. This detects whether Collectors are falling behind in sending events to Workers. This may be caused by Workers slow in ingesting events to storage or Collectors slow processing events and uploading to Workers.<br>• Normal - if nodes.metrics.lastEventTime less than 15 minute delay<br>• Warning - if nodes.metrics.lastEventTime between (15 minute and 20 minute) delay<br>• Critical - if nodes.metrics.collectorUploadStatus.lastEventTime more than 20 minute delay |
| Last File Received | Collector | This information is sent by each Worker to Supervisor based on what each Worker receives from Collectors. This may be caused by Workers slow in ingesting events to storage or Collectors slow processing events and uploading to Workers.<br>• Normal - if nodes.metrics.lastFileReceived less than 15 minute delay<br>• Warning - if nodes.metrics.lastFileReceived between (15 minute and 20 minute) delay<br>• Critical - if nodes.metrics.lastFileReceived more than 20 minute delay |