FortiSIEM - Integration API Guide

Version 5.2.5

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/support-and-training/training.html

NSE 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

10/11/2019
FortiSIEM 5.2.5 Integration API Guide

TABLE OF CONTENTS

Overview

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

These APIs are available for interacting with the FortiSIEM CMDB.

Add or Update an Organization

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

API Specifications

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:** `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/organization/add` • **Update an organization:** `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/organization/update`
Input Parameters	User name and password of Super account or Organization specific account, Organization definition file
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.

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.

API Specifications

Methodology	REST API based: Caller makes an HTTP(S) request with an input XML (optional).
Input URL	• **For adding or updating:** `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/deviceMaint/update` • **For deleting:** `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/deviceMaint/delete`
Input Parameters	An XML file Containing devices and maintenance calendar updates.
Input Credentials	User name and password of any FortiSIEM account with appropriate access control.
Output	An HTTP status code.

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

Create or Update Device Credentials

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

API Specifications

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.

Methodology	REST API based: Caller makes an HTTP(S) request with an input XML.
Request URL	`https://<FortiSIEM_Supervisor_IP>/phoenix/rest/deviceMon/updateCredential`
Input Parameters	• **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access. • **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.

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.

API Specifications

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:** `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/deviceMon/discover` • **Get Discovery result:** `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/deviceMon/status?taskId=XXX`
Input Parameters	• **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. • **Enterprise deployments:** User name and password of any FortiSIEM account that has the appropriate access.
Output	• Discovery request: XML containing task Id. • Discovery result: XML containing discovered devices and attributes.

Refer to Example Usage for discovering devices.

Get Agent Status for a Specific Host

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

API Specifications

Methodology	REST API based: Caller makes an HTTPS request with query parameters: `orgId`, `hostName`.
Request URL	`https://<FortiSIEM_Supervisor_IP>/phoenix/rest/agentStatus/all?request=<orgId>,<hostName>`

Input Credentials	User name and password of Super account or Organization-specific account.
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.

Get CMDB Device Info

This API enables you to get CMDB information in Enterprise and Service Provider deployments. The APIs for Service Provider deployments differ from the Enterprise deployments in that you must specify an organization for the input URL and credentials.

- Get Short Description of All Devices
- Get Short Description of All Devices in an Address Range
- Get Full Information about One Device
- Get a Section of Information (Applications, Interfaces, Processors, Storage) about One Device

Get Short Description of All Devices

Methodology	REST API based: Caller makes an HTTP(S) request with an input XML. An output XML is returned.
Input URL	• **Enterprise deployments:** `https://<<FortiSIEM_Supervisor_IP>/phoenix/rest/cmdbDeviceInfo/devices` • **Service Provider deployments:** `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/cmdbDeviceInfo/devices&organization=ACME`
Input Credentials	• **Enterprise deployments:** User name and password of any FortiSIEM account. Make sure that the account has the appropriate access. • **Service Provider deployments:** User name and password of any FortiSIEM account for the ACME organization. Make sure that the account has the appropriate access.
Output	An XML that contains a short set of attributes for each device, including: • Host Name • Access IP • Creation Method • Description • Vendor, Model, version • Contact info • Location • Uptime • Hardware Model

- Serial Number
- Business Service Groups to which the device belongs

Get Short Description of All Devices in an Address Range

Methodology	REST API based: Caller makes an HTTP(S) request with an input XML. An output XML is returned.
Input URL	• **Enterprise deployments:** `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/cmdbDeviceInfo/devices?includeIps=<includeIpSet>&excludeIps=<excludeIpSet>` • **Service Provider deployments:** `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. Make sure that the account has the appropriate access. • **Service Provider deployments:** User name and password of any FortiSIEM account for the ACME organization. Make sure that the account has the appropriate access.
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: `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: `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

Methodology	REST API based: Caller makes an HTTP(S) request with an input XML (optional). An output XML is returned.
Input URL	• **Enterprise deployments:** `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/cmdbDeviceInfo/device?ip=<deviceIp>&loadDepend=true` • **Service Provider deployments:** `https://<FortiSIEM_Supervisor_IP>/phoenix/rest/cmdbDeviceInfo/device?ip=<deviceIp>&loadDepend=true&organization=ACME`
Input Credentials	• **Enterprise deployments:** User name and password of any FortiSIEM account. Make sure that the account has the appropriate access. • **Service Provider deployments:** User name and password of any FortiSIEM account for the ACME organization. Make sure that the account has the appropriate access.
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

Methodology	REST API based: Caller makes an HTTP(S) request with an input XML (optional). An output XML is returned.
Input URL	• **Enterprise deployments:** `https://<FortiSIEM_Supervisor_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. Make sure that the account has the appropriate access. • **Service Provider deployments:** User name and password of any FortiSIEM account for the ACME organization. Make sure that the account has the appropriate access.
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 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.

API Specifications

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/deviceInfo/monitoredDevices`
Input Credentials	• **Enterprise deployments:** User name and password of any FortiSIEM account. • **Service Provider deployments:** User name and password of Super account or Organization specific account, 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.

Get the List of Monitored Organizations

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

API Specifications

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	User name and password of Super account.
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.

Update Device Monitoring

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

API Specifications

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. • **Service Provider deployments:** User name and password of Super account or Organization specific account, Organization name, input XML containing the updates to device monitoring configuration.
Input Parameters	User name and password of Super Global account or Organization specific account, Organization name, input XML containing the updates to device monitoring configuration.
Output	HTTP Status Code

Refer to Example Usage for updating device monitoring.

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

Input URL	`https://<Accelops_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 • **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.
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.

Input URL	`https://<Accelops_IP>/phoenix/rest/query/progress/<queryId>`
Output	progress (pct) 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

Input URL	`https://<Accelops_IP>/phoenix/rest/query/events/<queryId>/<begin>/<end>`
Output	totalCount (first time) and an XML containing the incident attributes. 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.

Incident Notification Integration

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

These topics describe the notification types:

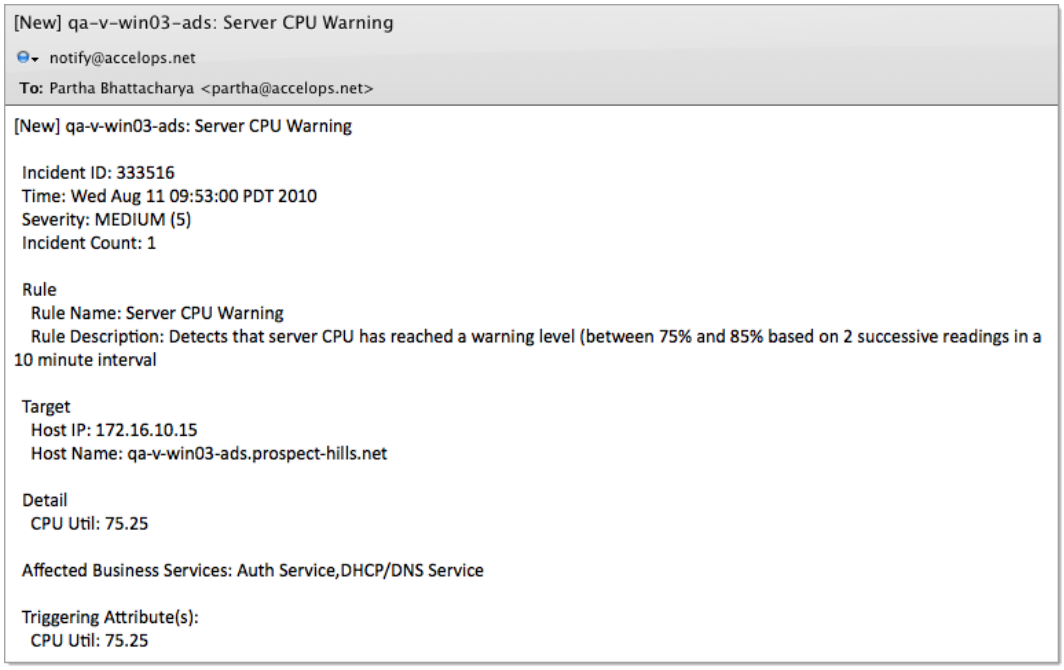
- Email/SMS
- HTTPS
- SNMP Trap
- API
- Get Triggering Event IDs for One or More Incidents

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.

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

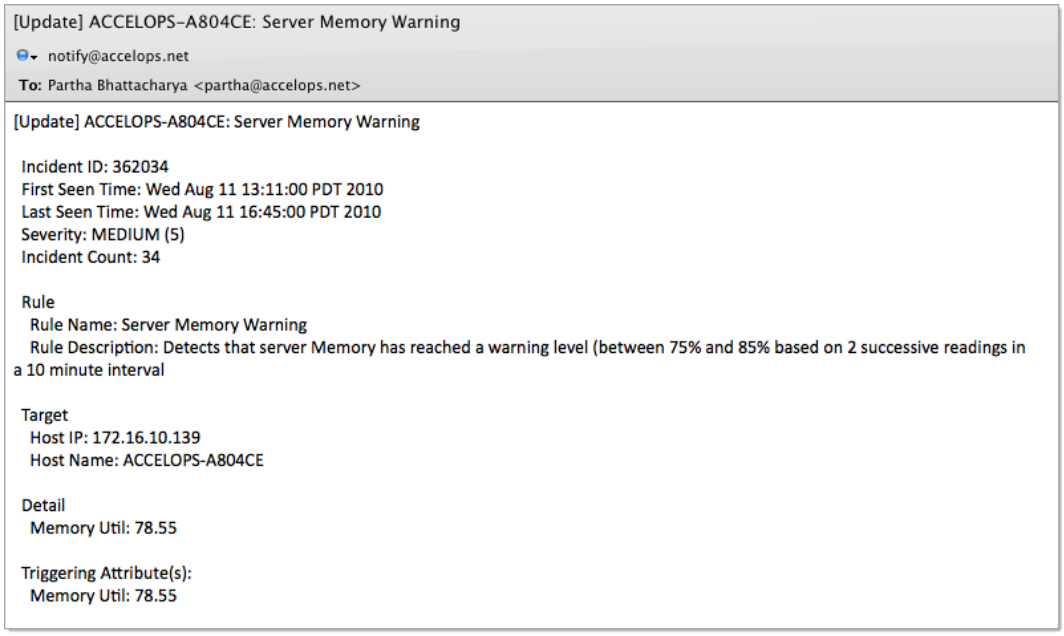
Target
Host IP: 172.16.10.15
Host Name: qa-v-win03-ads.prospect-hills.net

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

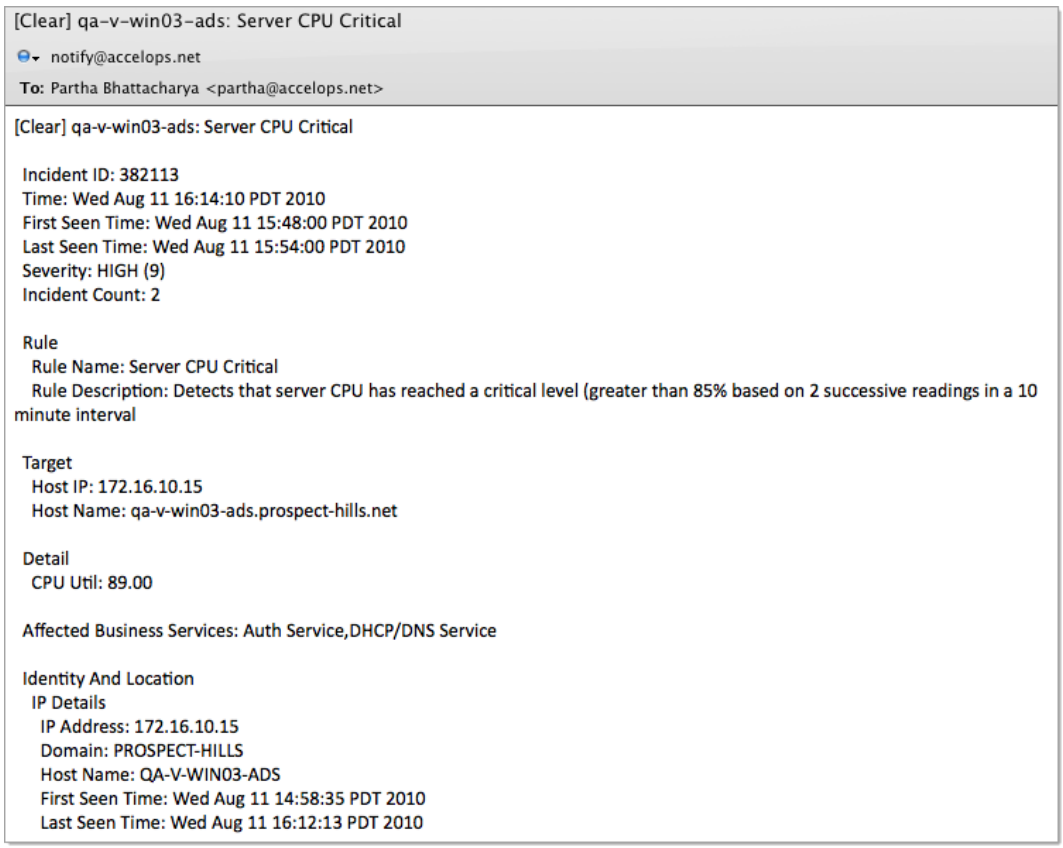
Rule
Rule Name: Server Memory Warning
Rule Description: Detects that server Memory has reached a warning level (between 75% and 85% based on 2 successive readings in a 10 minute interval

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

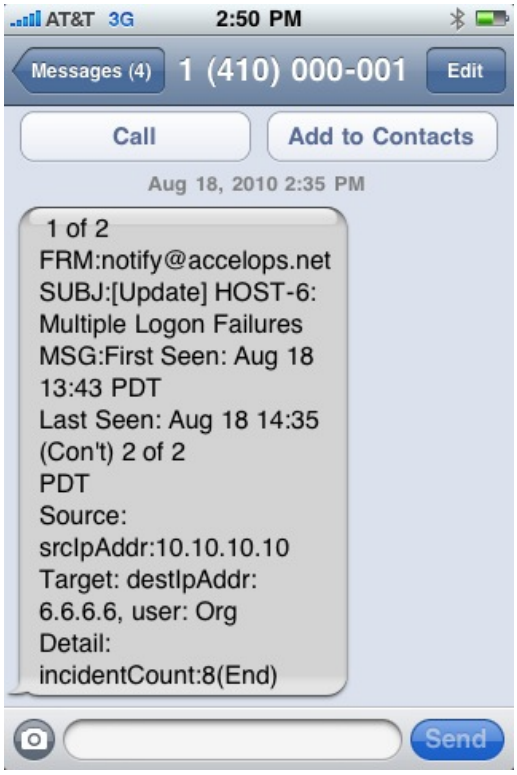
```
[New|Update|Clear] <HostName>: <Rule Name>
```

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. - Host name - User - Domain - Nearest switch name/port or VPN gateway or Wireless Controller - 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.



Notifications via HTTPS

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

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
	organization	The name of the organization for which this

Section	Field	Description
		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. • ipAddr

Section	Field	Description

		• hostName
		• vendor
		• model
		• version
		• users - Logged on users using this IP info obtained from Active Directory
		  • userName - Active Directory login name
		  • fullName - Full name of this user in Active Directory or defined manually
		  • email - email address of the user in Active Directory or defined manually
		  • jobTitle - jobTitle of the user in Active Directory or defined manually
		  • 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 to configure your device to handle SNMP traps sent from FortiSIEM.

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

Input URL	`https://<FortiSIEM_Supervisor_IP>/phoenix/rest/query/eventQuery`
Input Parameters	XML file containing the query parameters
Input Credentials	• **Enterprise deployments**: Username and password of any FortiSIEM account • **Service Provider deployments**: Username 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.
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.

Input URL	`https://<FortiSIEM_Supervisor_IP>/phoenix/rest/query/progress/<queryId>`
Output	progress (pct) 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

Input URL	`https://<FortiSIEM_Supervisor_IP>/phoenix/rest/query/events/<queryId>/<begin>/<end>`
Output	totalCount (first time) and an XML containing the incident attributes. 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,incidentL
astSeen,eventSeverity,incidentTicketUser,hostIpAddr,eventName,phEventCategory,inci
dentTicketId,count,incidentDetail,incidentSr
```

```
c,eventSeverityCat,incidentFirstSeen,incidentViewUsers,incidentComments,incidentCl
earedUser,incidentNoti
Recipients,incidentId,phRecvTime,incidentStatus,incidentViewStatus,incidentTarget,
incidentRptIp
```

Incident Notification XML Schema

The following is the schema for incident notification output file:

```
<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

Methodology	REST API based: Caller makes an HTTPS request with query parameter: `incidentId`.
Request URL	`https://<FortiSIEM_SupervisorIP>/phoenix/rest/incident/triggeringEvents?incidentIds=<incidentId1>,<incidentId2>`
Input Credentials	User name and password of Super account or Organization-specific account.
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.

Incident Update

Update Incident Attributes

This API enables you to update certain incident attributes.

API Specifications

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	User name and password of Super account or Organization specific account
Input JSON	**ContentType:** `application/json` **RequestPayload:** `{"incidentId":"1","comments":"XYZ","incidentStatus":"3","externalTicketType":"MEDIUM","externalTicketId":"1111","externalTicketState":"CLOSED","externalAssignedUser":"ABC"}` • `incidentId` – Incident ID for the incident to be updated • `comments` – Any comments • `incidentStatus` – 0 (Active), 1 (Auto Cleared), 2 (Manually Cleared), or 3 (System Cleared) • `externalTicketType` – Low, Medium, or High • `externalTicketId` – External Ticket ID • `externalTicketState` – New, Assigned, In Progress, or Closed • `externalAssignedUser` – External Assigned User
Output	HTTP status code

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

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.

API Specifications

Methodology	REST API based: Caller makes an HTTP(S) request with an input XML.
Request URL	**Add a Dashboard folder to an Organization:** `https://<FortiSIEM_Supervisor_ IP>/phoenix/rest/dashboard/html/add`
Input Parameters	User name and password of Super account or Organization specific account and Dashboard folder definition file.
Input XML	Contains dashboard details to be included in this folder: - Dashboard folder name - Organization name - Time range - Dashboard type
Output	An HTTP status code.

Refer to Example Usage for adding a Dashboard folder.

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 section of the Fortinet Support website https://support.fortinet.com.

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 section of the Fortinet Support website https://support.fortinet.com.

Example Usage

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

https://filestore.fortinet.com/docs.fortinet.com/v2/resources/FortiSIEM-RestAPI-525.zip

Python Support

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