

FSO Plugin Scoping Workbook

LogRythm Platform Manager v1.0.0

February 22, 2022

# Table of Contents

[Table of Contents 2](#_Toc470609371)

[Scoping Questions 3](#_Toc470609372)

[Integration Target 3](#_Toc470609373)

[Use Cases 4](#_Toc470609374)

[Device Parameters 4](#_Toc470609375)

[Commands 5](#_Toc470609376)

[queryAlarmsService 5](#_Toc470609377)

[Complex Objects 6](#_Toc470609378)

[LogRythmAlarm 6](#_Toc470609379)

# Scoping Questions

The following questions are used to help scope the potential ROI for automation and help stimulate discussion about techniques to achieve the desired results through existing mechanisms or process improvements.

|  |  |
| --- | --- |
| Question | Response |
| What categories best describe the use cases for the plugin? | SIEM |
| Approximately how much time is currently spent by analysts on the above activities on a per case basis? | 10-20 minutes |
| Approximately how often do analysts perform the above use cases? | 20-30 times per day |
| What mechanisms can the target product use to receive information to ingest or action commands? | Web API |
| What mechanisms can the target product use to send event and alert information back to the orchestration platform? | Web API |
| Does the integration require querying events in the target product? | Yes |
| Does the integration require sending action commands to the target product? | Yes |
| Does the product send events and activity logs to a SIEM or central log management solution where orchestration could collect them? | LogRhythm v7.5.0 |
| Does the target product have a documented API ? | Accessible only through the customer portal |

# Integration Target

The following table summarizes the third party product with which the FSO plugin will integrate.

|  |  |
| --- | --- |
| Item | Detail |
| Product Vendor | LogRhythm |
| Product Name | Platform Manager |
| Product Version | V7.5.0 |
| API name (if applicable) | LRAPI\_7.5.0 |
| API Version | 7.5.0 |

# Use Cases

The following table outlines the expected common use cases for the plugin.

|  |  |
| --- | --- |
| Use Case Title | Description |
| queryAlarmsAdapter | Periodically check for new alarms and return their summary as cases with FSO for further orchestration |
| queryAlarmById | Query for alarm summary given an AlarmId |
| getEventsByAlarmId | Get events associated with an alarm given its Id |
| updateAlarmStatus | Update status of an alarm given AlarmId & status |
| createCase | Create a case in Logrhythm Case Manager |

# Device Parameters

The following parameters will be required by FSO when a user creates a new device instance of the target product. The parameters will be available to all commands for the unique instance of the device within FSO. For example, a web API will typically require hostname, username and password in order for FSO to connect to it. A plugin that only does local processing may not need device parameters.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name | Description | Type | Optional | Default Value | Encrypted |
| Hostname | Hostname of LogRhythm SOAP API web server | HostName | False |  | False |
| VerifySSL | Perform SSL certificate verification | Bool | False | True |  |
| Username | Username | UserName | False |  | False |
| Password | password | String | False |  | True |
| BasicAuth | Select if Windows Authentication is not required | Bool | False | True |  |
| CaseAPIUrl | Base url for logrhythm’s case API, e.g. <https://localhost:8501> | URL | False |  |  |
| CaseAPIKey | API key for accessing logrhythm’s case API | String | False |  | True |

# Commands

These represent the actions blocks that will be available in the CoA builder. Each action will have input parameters and output parameters. The action and target names will appear in the CoA builder block for the command. The manual time is the time required by a human-based process to complete the desired action. If this command will run automatically at specified intervals to retrieve events or if it will listen on the network for an inbound event, then it will need to be an adapter command.

The following table summarizes the commands that are to be defined in the plugin.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Command Name | Description | Action Name | Target Name | Manual Time | Is Adapter |
| queryAlarmsAdapter | Periodically check for new alarms and return their summary as cases with FSO for further orchestration | Query | Alarm Service |  | True |
| queryAlarmById | Query for alarm summary given an AlarmId | Query | Alarms |  | False |
| getEventsByAlarmId | Get events associated with an alarm given its Id | Get | Events |  | False |
| updateAlarmStatus | Update status of an alarm given AlarmId & status. | Update | Alarm Status |  | False |
| createCase | Create a case in Logrhythm Case Manager | Create | Case |  | False |

Each of the commands from the above table are further defined in their respective sections below.

## queryAlarmsAdapter

### Input Parameters

If a parameter is optional, then FSO will allow the parameter to be omitted or left empty during command configuration, and its absence will not prevent command execution.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name | Description | Type | Optional | Default Value | Encrypted |
| startDate | Start date for the data query | DateTime | False |  |  |
| endDate | End date for the data query | DateTime | False |  |  |
| allUsers | If true, alarms for all users | Bool | False |  |  |
| maximumResultsPerPage | The maximum number of rows the response can contain, regardless of the actual number of rows returned. | Integer | False | 100 |  |
| rawOnly | If rawOnly is True, only rawResult will be provided, alarmSummary won’t be provided, else both will be provided. | Bool | False | False |  |

### Output Parameters

If a parameter is optional, then FSO will not consider the command to have failed if the optional parameter is omitted or left empty in the plugin output.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Description | Type | Optional | Default Value |
| rawResult | Raw result returned by logrhythm API | String | False |  |
| alarmSummary | Response model for alarm summary | AlarmSummaryData | True |  |

## queryAlarmById

### Input Parameters

If a parameter is optional, then FSO will allow the parameter to be omitted or left empty during command configuration, and its absence will not prevent command execution.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name | Description | Type | Optional | Default Value | Encrypted |
| alarmId | Unique Id associated with alarm | Integer | False |  |  |
| rawOnly | If rawOnly is True, only rawResult will be provided, alarmSummary won’t be provided, else both will be provided. | Bool | False | False |  |

### Output Parameters

If a parameter is optional, then FSO will not consider the command to have failed if the optional parameter is omitted or left empty in the plugin output.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Description | Type | Optional | Default Value |
| rawResult | Raw result returned by logrhythm API | String | False |  |
| alarmSummary | Response model for alarm summary | AlarmSummaryData | True |  |

## getEventsByAlarmId

### Input Parameters

If a parameter is optional, then FSO will allow the parameter to be omitted or left empty during command configuration, and its absence will not prevent command execution.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name | Description | Type | Optional | Default Value | Encrypted |
| alarmId | Unique Id associated with alarm | Integer | False |  |  |
| rawOnly | If rawOnly is True, only rawResult will be provided, eventSummary won’t be provided, else both will be provided. | Bool | False | False |  |

### Output Parameters

If a parameter is optional, then FSO will not consider the command to have failed if the optional parameter is omitted or left empty in the plugin output.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Description | Type | Optional | Default Value |
| rawResult | Raw result returned by logrhythm API | String | False |  |
| eventSummary | Response model for event summary | EventSummaryData | True |  |
| alarmId | Alarm Id for which events are being fetched, can be used for downstream tasks | Integer | False |  |

## updateAlarmStatus

### Input Parameters

If a parameter is optional, then FSO will allow the parameter to be omitted or left empty during command configuration, and its absence will not prevent command execution.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name | Description | Type | Optional | Default Value | Encrypted |
| alarmID | The unique ID of the alarm | Integer | False |  |  |
| status | Status to be set/updated | String | False |  |  |
| comments | Reason for alarm update(optional) | String | True |  |  |

Status can be one of – New, Opened, Working, Escalated, Closed, Closed\_FalseAlarm, Closed\_Resolved, Closed\_Unresolved, Closed\_Reported, Closed\_Monitor

### Output Parameters

If a parameter is optional, then FSO will not consider the command to have failed if the optional parameter is omitted or left empty in the plugin output.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Description | Type | Optional | Default Value |
| updateAlarmResult | Response model for alarm summary | UpdateAlarmResult | false |  |

## createCase

### Input Parameters

If a parameter is optional, then FSO will allow the parameter to be omitted or left empty during command configuration, and its absence will not prevent command execution.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name | Description | Type | Optional | Default Value | Encrypted |
| externalId | Externally defined identifier for the case | String | False |  |  |
| name | Name of the case | String | False |  |  |
| priority | Priority of the case. Can take values 1 to 5. | Integer | False |  |  |
| dueDate | When the case is due, as an RFC 3339 formatted string | String | False |  |  |
| summary | Note summarizing the case | String | False |  |  |
| entityId | Entity to assign to the case | Integer | False |  |  |

### Output Parameters

If a parameter is optional, then FSO will not consider the command to have failed if the optional parameter is omitted or left empty in the plugin output.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Description | Type | Optional | Default Value |
| createCaseResponse | Response model for Create Case | CreateCaseResponse | false |  |
| Success | True is successfully created | Bool | false |  |

# Complex Objects

If the use case calls for it, the data returned from the commands inside the plugin be parsed and normalized into these data objects. This will leverage FSO’s validation features to ensure that each of the objects attributes are of the expected type.

## AlarmSummaryData

|  |  |  |
| --- | --- | --- |
| Name | Description | Type |
| AlarmID | The unique ID of this instance of an alarm. | Long |
| EntityID | The unique ID of this entity associated to this instance of an alarm. | Int |
| EntityName | The name of the entity associated to this instance of an alarm. | String |
| LastUpdatedID | The unique ID of the change set for the last update of this instance of the alarm | Int |
| LastUpdateName | The name of the Person who last updated this instance of alarm | String |
| AlarmRuleID | The unique ID of Alarm Rule associated to this instance of Alarm | Int |
| AlarmRuleName | The name of Alarm Rule associated to this instance of alarm | String |
| AlarmStatus | The current alarm status of this instance of alarm | String |
| EventCount | The number of events associated with this instance of alarm | Int |
| EventDateFirst | The first normalized date time of an event associated with this instance of alarm | dateTime |
| EventDateLast | The first normalized date time of an event associated with this instance of alarm | dateTime |
| RBPAvg | The average risk based priority of all events which generated this instance of the alarm | Int |
| RBPMax | The max risk based priority of all events which generated this instance of the alarm | Int |
| AlarmDate | The normalized date time which this instance of alarm was generated | dateTime |
| DateInserted | The normalized date time which this instance of alarm was generated | dateTime |
| DateUpdated | The normalized date time that the comments or status of this instance of alarm was updated | dateTime |

## UpdateAlarmResult

|  |  |  |
| --- | --- | --- |
| Name | Description | Type |
| Succeeded | A flag indicating whether the update succeeded or failed | Bool |
| DataID | The unique ID of the data artifact which were updated | Long |
| Errors | The tabular errors object of all errors associated to this save result | ErrorInfo.list |
| Warnings | The tabular warning object of all warnings associated to this save result | String.list |

## ErrorInfo

|  |  |  |
| --- | --- | --- |
| Name | Description | Type |
| ErrorID | The unique ID of error details | int |
| Details | The error details for this instance of error | String |
| ErrorMessage | The error message of the error | String |

## EventSummaryData

|  |  |  |
| --- | --- | --- |
| Name | Description | Type |
| Account | User account referenced or impacted by log activity. | String |
| Amount | Amount of an item. | Float |
| Bytes | Amount of data sent and received from a device, system or process | Float |
| BytesIn | Number of bytes received or input from a device, system or process | Float |
| BytesOut | Number of bytes sent from a device, system or process | Float |
| ClassificationID | The unique ID of one of three major ctivity groups–Operations, Audit, or Security–and a more specific sub-classification. | Integer |
| Command | The command that was executed. | String |
| CommonEventId | The unique ID of the common event which determines its Classification. | Integer |
| CommonEventName | A short, plain-language description of the log that determines its Classification. | String |
| Count | The number of times the log entry occurred when aggregated with other identical log entries. | Integer |
| Direction | The enumeration of the Direction of activity between a log's Origin and Impacted Zones. | String |
| DirectionName | Direction by name of activity between a log's Origin and Impacted Zones. Values can be Internal, External, Outbound, Local, or Unknown. | String |
| Domain | Windows of DNS referenced or impacted by log activity. | String |
| Duration | Running time of a session, job, activity, etc. | Float |
| EntityID | The unique ID of the entity. | Integer |
| EntityName | The name of the entity. | String |
| Group | User group or role referenced or impacted by log activity. | String |
| ImpactedEntityId | The unique ID of the Impacted Entity. | Integer |
| ImpactedEntityName | The resolved Entity of the impacted host. | String |
| ImpactedHostId | The unique ID of the Host such as a DNS name or NetBIOS impacted by the log activity. | Integer |
| ImpactedInterface | The impacted interface number of a device or the physical port number of a switch. | String |
| ImpactedIP | The IP address impacted by the log activity. | String |
| ImpactedHostName | The name of the Host such as a DNS name or NetBIOS name impacted by the log activity. | String |
| ImpactedLocationID | The unique ID of the Impacted Location object. | Integer |
| ImpactedMAC | The host/device impacted MAC address. | String |
| ImpactedName | The device name impacted. | String |
| ImpactedNATIP | The IP address the Impacted IP was translated to/ from via NAT device logs. | String |
| ImpactedNATPort | The TCP/UDP address the Impacted IP was translated to/from via NAT device logs. | Integer |
| ImpactedNetworkId | The unique ID for the Known Network that was impacted by the log activity. | Integer |
| ImpactedPort | The destination/client TCP/UDP port number. | Integer |
| ImpactedZone | The enumeration value of the resolved Zone that was impacted by the activity - Internal, External or DMZ. | String |
| ImpactedZoneName | The name of this specific zone. | String |
| ItemsPacketsIn | Items such as packets received or input from a device, system or process | Float |
| ItemsPacketsOut | Items such as packets sent or output from a device, system or process | Float |
| LogDate/NormalDate | Timestamp when the log was generated or received, corrected to UTC. | DateTime |
| LogMessage | The log message generated due to the activity detected by the source. | String |
| Login | User associated with the log activity. | String |
| LogSourceHost | The system or device where the Log Source originates. | String |
| LogSourceHostId | The unique ID of the log source host object. | Integer |
| LogSourceHostName | The name of the log source host. | String |
| LogSourceId | The unique ID of the log source. | Integer |
| LogSourceName | A unique log originator on a specific Host. | String |
| LogSourceType | Type of facility or source where the log originated. | Integer |
| LogSourceTypeName | Type of facility or source where the log originated. | String |
| MessageID | The unique ID for this log Message. | Integer |
| MessageType | The Message Type that could be: Message, Log, Known Log, Event, Alarm. | String |
| MPERuleId | The unique ID of the associated MPE Rule object. | Integer |
| MPERuleName | Message Processing Engine (MPE) Rule. It identifies and normalizes a log messages and assigns it a Common Event. | String |
| NormalDateMax | If message is aggregated the max creation date contained in the group of logs. It can be in UTC or user-selected time zone. | DateTime |
| Object | Resource such as a file, file path, or registry key that is referenced or impacted by log activity. | String |
| ObjectName | Name of the resource such as a file, file path, or registry key that is referenced or impacted by log activity. | String |
| OriginEntityId | The unique ID of the Origin Entity. | Integer |
| OriginEntityName | The resolved Entity of the origin host. | String |
| OriginHostId | The unique ID of the Origin Host object. | Integer |
| OriginInterface | The origin interface number of a device or the physical port number of a switch. | String |
| OriginIP | The IP address that was the origin of the log activity. | String |
| OriginHostName | The name of the Host such as a DNS name or NetBIOS name that was the origin of the log activity. | String |
| OriginLocationID | The unique ID of the Origin Location object. | Integer |
| OriginLogin | User associated with the log activity. | String |
| OriginMAC | The host/device origin MAC address. | String |
| OriginName | The orgin of the transaction captured by the log. | String |
| OriginNATIP | The IP address the Origin IP was translated to/ from via NAT device logs. | String |
| OriginNATPort | The TCP/UDP address the Origin IP was translated to/from via NAT device logs. | Integer |
| OriginNetworkId | The unique ID of the Origin Network object. | Integer |
| OriginPort | The source/client TCP/UDP port number. | Integer |
| OriginZone | The enumeration value of the resolved Zone that was the origin of the activity - Internal, External or DMZ. | String |
| OriginZoneName | The name given to this specific zone. | String |
| Priority | Calculated Risk Based Priority (RBP) of the log entry. | Integer |
| Process | Name or value that identifies a process. | String |
| ProcessID | The unique ID of the process object. | Integer |
| ProtocolId | The unique ID of the Protocol object. | Integer |
| ProtocolName | Network protocol applicable to the log message. | String |
| Quantity | The item quantity. | Float |
| Rate | Rate of an item. | Float |
| Recipient | Email address or VOIP caller number. For non- email logs, it might represent who received some form of information. | String |
| Sender | Email originator or VOIP caller number. For non- email logs, it might represent who received some form of information. | String |
| SequenceNumber | The collection sequence of events obtained to generate an alarm. | Integer |
| ServiceId | The unique ID of the Service object. | Integer |
| ServiceName | The name of a service which transferred the recorded traffic. | String |
| Session | User, system or application session | String |
| Severity | Value indicating severity of the log. | String |
| Size | Item Size. | Float |
| Subject | Email subject line. For other logs, it might represent the subject of some form of communicated information. | String |
| URL | URL referenced or impacted by log activity. | String |
| VendorMsgID | Unique, vendor-assigned value that IDs the log message. | String |
| Version | Value representing the version (i.e., OS version, patch version, doc version, etc.). | String |
| ClassificationName | The name of one of three major activity groups– Operations, Audit, or Security–and a more specific sub-classification. | String |
| ClassificationTypeName | One of three major activity groups: Operations, Audit, or Security. | String |
| ImpactedLocation | Country, region, and/or city impacted by the logged activity as derived from the GeoIP resolution. | LocationInfoDataModel |
| OriginLocation | Known Network that was the origin of the log activity. | LocationInfoDataModel |
| ImpactedNetwork | Known Network that was impacted by the log activity. | NetworkDataModel |

## LocationInfoDataModel

|  |  |  |
| --- | --- | --- |
| Name | Description | Type |
| CityName | The city name of the GeoIP location resolved for this address. | String |
| CountryName | The country name of the GeoIP location resolved for this address. | String |
| FullName | The full name of the GeoIP location resolved for this address. | String |
| FullNameRegion | The region full name of the GeoIP location resolved for this address. | String |
| HasCity | If true | Bool |
| HasCountry | If true | Bool |
| HasLatLong | If true | Bool |
| HasParentLocation | If true | Bool |
| HasRegion | If true | Bool |
| IsValid | If true | Bool |
| Latitude | The latitude of the GeoIP location resolved for this address. | Float |
| LocationID | The unique ID of the location object. | Integer |
| LocationKey | The location abbreviation used on some displays. | String |
| Longitude | The longitude of the GeoIP location resolved for this address. | Float |
| ParentLocationID | The unique ID of the parent location object. | Integer |
| RegionName | The region name of the GeoIP location resolved for this address. | String |
| Type | The location type of the GeoIP location resolved for this address. | String |

## NetworkDataModel

|  |  |  |
| --- | --- | --- |
| Name | Description | Type |
| DestinationRiskLevel | The destination risk level assigned to this network. | Integer |
| DestinationRiskLevelName | The destination risk level name assigned to this network. | String |
| DisplayValue | The display value. | String |
| EntityID | The unique ID for the entity object. | Integer |
| HasLocationID | If true, the network has a location association. | Bool |
| HasLocationKey | If true, the network has a location key association. | Bool |
| HostZone | The host zone object associated to the network. | String |
| HostZoneName | The host zone name associated to the network. | String |
| LocationID | The unique ID for location object. | Integer |
| LocationKey | The location key for the network. | String |
| NetworkId | The unique ID for the network object. | Integer |
| SourceThreatLevel | The source threat level assigned to the network. | Integer |
| WatchLevelName | The watch level name assigned to the network. | String |
| BeginIPRange | The beginning value of the IP range of the network. | IPAddressDataModel |
| EndIPRange | The ending value of the IP address range for the network. | IPAddressDataModel |
| WatchLevel | The watch level assigned to the network. | WatchItemDataModel |

## IPAddressDataModel

|  |  |  |
| --- | --- | --- |
| Name | Description | Type |
| Bytes | The byte length of the IP object value. | String |
| Value | The IP address value. | String |
| IsBroadcast | If true, this is a broadcast address. | Bool |
| IsIPv4 | If true, this is an IPv4 address. | Bool |
| IsIPv6 | If true, this is an IPv6 address. | Bool |
| IsLinkLocal | If true, this is a link local address. | Bool |
| IsLoopback | If true, this is a loopback address. | Bool |
| IsNetwork | If true, this is a network address. | Bool |
| IsPrivate | If true, this is private address. | Bool |
| IsPublicIPv4 | If true, this is a public IPv4 address. | Bool |
| IsResolvable | If true, the address is resolvable. | Bool |

## WatchItemDataModel

|  |  |  |
| --- | --- | --- |
| Name | Description | Type |
| Comments | The comments set on a watch item. | String |
| HostID | The unique ID of the requested host for this watch item. | Integer |
| Login | The login of the request account for this watch item. | String |
| NetworkId | The unique ID for the network for this watch item. | Integer |
| PersonID | The unique ID for the person for this watch item. | Integer |
| WatchItemType | The enumeration of the type of watch item. | String |
| WatchLevel | The enumeration of the watch level requested. | String |
| WatchLevelName | The name of the watch level requested. | String |

## CreateCaseResponse

|  |  |  |
| --- | --- | --- |
| Name | Description | Type |
| id | Unique identifier for the case, as an RFC 4122 formatted string | String |
| number | Unique, numeric identifier for the case | Integer |
| externalId | Externally defined identifier for the case | String |
| dateCreated | When the case was created, as an RFC 3339 formatted string | String |
| dateUpdated | When the case was updated, as an RFC 3339 formatted string | String |
| dateClosed | When the case was closed, as an RFC 3339 formatted string | String |
| owner | Owner details | User |
| lastUpdatedBy | Last Updated by | User |
| name | Name of the case | String |
| priority | Priority of the case | Integer |
| dueDate | When the case is due, as an RFC 3339 formatted string | String |
| status | Status | Status |
| resolution | Description of how the case was resolved | String |
| resolutionDateUpdated | When the case resolution was last updated, as an RFC 3339 formatted string | String |
| resolutionLastUpdatedBy | Resolution Last Updated by | User |
| summary | Note summarizing the case | String |
| entity | Entity associated with the case | Entity |
| collaborators | List of collaborators on the case | User.list |
| Tags | List of tags added to the case | Tag.list |

## User

|  |  |  |
| --- | --- | --- |
| Name | Description | Type |
| number | Unique, numeric identifier for the person | Integer |
| name | Name of the person | String |
| Disabled | If the person is disabled in the system | Bool |

## Entity

|  |  |  |
| --- | --- | --- |
| Name | Description | Type |
| number | Unique, numeric identifier for the entity | Integer |
| name | Name of the Entity | String |
| fullName | Parent Entity/Child Entity | String |

## Status

|  |  |  |
| --- | --- | --- |
| Name | Description | Type |
| number | Numeric identifier of the status | Integer |
| name | Display Name for status | String |

## Tag

|  |  |  |
| --- | --- | --- |
| Name | Description | Type |
| number | Unique, numeric identifier for the tag | Integer |
| text | Tag text | String |

# Future Scope

These are the additional functionalities which can be provided alongside this plugin. These features are beyond the scope of v1.0.0 of the Logrhythm Platform Manager Plugin and these may be included in the future releases of this plugin.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Command Name | Description | Action Name | Target Name | Manual Time | Is Adapter |
| updateCase | Update a particular Case using logrhythm’s Case API | Update | Case |  | False |
| getCase | Get details of a particular Case using logrhythm’s Case API | Get | Case |  | False |
| updateCaseStatus | Update status of a particular Case using logrhythm’s Case API | Update | Case Status |  | False |