

FSO Plugin Scoping Workbook

THREATQUOTIENT

March 16, 2022

# Table of Contents

Table of Contents ---------------------------------------------------------------------------------------------------------------2

Use Cases ------------------------------------------------------------------------------------------------------------------------3

Device Parameters --------------------------------------------------------------------------------------------------------------3

Commands -------------------------------------------------------------------------------------------------------------------------4

listIndicators--------------------------------------------------------------------------------------------4

queryIndicators-----------------------------------------------------------------------------------------5

createIndicators----------------------------------------------------------------------------------------6

# Use Cases

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

|  |  |
| --- | --- |
| Use Case Title | Description |
| listIndicators | Retrieve a list of indicators |
| queryIndicators | Querying for specific indicator values |
| createIndicator | Creating an indicator |

# 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 |
| email | Email | String | False |  |  |
| password | password | String | False |  | True |
| client\_ID |  | String | False |  |  |
| VerifySSL | Perform SSL certificate verification | Bool | False | True |  |

# listindicators

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 |
| limit | Use this param to limit the result | 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 |
| rawJSON | Raw response in JSON format | JSON | False |  |
| statusMsg | Status message of the response | String | False |  |
| success | Status of response | bool | False |  |

# QUERYindicators

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 |
| value | Use this URL param to query specific indicator | String | False |  |
| with | To return more fields beyond the basic ones, we can include a **with** URL parameter to specify the additional data fields we want to include. Options for this endpoint include adversaries, attachments, attributes, comments, events, indicators, score, signatures, sources, status, tags, type, and watchlist | String.list | True |  |

### 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 |
| rawJSON | Raw response in JSON format | JSON | False |  |
| statusMsg | Status message of the response | String | False |  |
| success | Status of response | bool | False |  |

# createindicator

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 |
| Indicator\_data | create a JSON file that will contain the basic indicator details: the indicator value, the type of indicator, the indicator’s status and the source of the indicator | String | 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 |
| statusMsg | Status message of the response | String | False |  |
| success | Status of response | bool | False |  |