LOGPOINT

Director

API Documentation

V2.7.0

CONTENTS

The API Server is the management platform for the LogPoint Director setup which consists of a user interface and a set of APIs. It exposes RESTful APIs to manage the configuration settings of the Fabric-enabled LogPoints.The Director Console APIs allows you to configure and manage the configuration settings of the Fabric-enabled LogPoints. You can use the Director Console API to configure the settings using a set of APIs and their endpoints.

ACCESSING THE API ENDPOINTS

For accessing each API endpoints, authentication tokens must be provided in the header in format 'Authorization: Bearer token'. The token can be generated from the Director Console Web Application.

Sample Request

```
curl -i
-H 'Authorization: Bearer
↪c3FlOG9vSGV4VHo4QzAyg5T1JvNnJoZ3ExaVNyQWw6WjRsanRKZG5lQk9q'
-H 'Content-Type: application/json'
-X POST
-d '{"data": {}}'
"https://api-server-host-name/configapi/v1/{pool_UUID}/{logpoint_identifier}/
↪BackupAndRestore/backupnow
```

CHAPTER

TWO

CONVENTIONS FOR NON-BREAKING AND BREAKING CHANGES

The Director Console API uses the following conventions to consider a change as non-breaking or a breaking change:

2.1 Non-Breaking Changes

- A new resource or API endpoint
- A new optional parameter
- A new optional key in the JSON POST body
- A new key returned in the JSON response body

2.2 Breaking Changes

- All changes except the non-breaking mentioned above. For example,
- A new required parameter
- A new required key in POST body
- Removal of a mandatory property (a key that is mandatory when creating the entity) from the response
- Renaming a property in a response. For example: changing 'device_name' to 'name'
- Changing a response to respond with an unexpected type. For example: changing 'hostname' type from String to List
- Removal of an existing endpoint
- Removal of an existing endpoint request method

- A substantially different internal behavior of an API call – such as a change to the default behaviour

CHAPTER

THREE

GUIDELINES FOR DIRECTOR CONSOLE API CLIENTS

3.1 General Guidelines

- Do safely ignore unknown and unexpected data in API responses
- Do safely ignore additional fields and object attributes in API responses
- Some services MAY add fields to responses without changing versions numbers. Services that do so MUST make this clear in their documentation and clients MUST ignore unknown fields
- Avoid relying on the order in which data appears in API JSON responses, unless order is explicitly defined as part of the service contract.
- Make sure that you call the RefreshList endpoint (if provided) for all the APIs after making updates to the configuration. This is to ensure that the API returns the latest data while using Get or List endpoints.

3.2 API Usage Guidelines

1. How to obtain Bearer Token?

   Bearer token can be obtained from Director Console's left navigation bar's Profile tab by clicking on *Generate Token* option. The token is valid only for 8 hours from the time it is generated. For times when the script runs for an extended period, you can use the Refresh Token API to obtain the new token automatically once the existing token expires.

2. How to obtain pool_UUID of the Fabric-enabled LogPoint?

   The value of the pool_UUID parameter can be obtained by logging into the Logpoint Search Master(LPSM) and navigating to the *Settings >> Configurations >> LogPoint Pool* section. Here a list of LPSM pools are displayed, and you can select the pool_UUID(UUID) by their Pool Name from the UUID column.

3. How to obtain logpoint_identifier?

   The value of the logpoint_identifier parameter be obtained by logging into Logpoint Search Master(LPSM) and navigating to the *Settings* >> *Configurations* >> *LogPoint Pool* section. You can find the details of all Fabric-enabled LogPoints associated with the pool by clicking on the Details icon under the Actions column. Click on the Details icon and find the name of your LogPoint and its identifier.

4. Since *add*, *edit* and *delete* operations are asynchronous, it might take some time to process them. Hence, a GET request might not always return the latest data. Also, if a Director console API request (PUT/POST/DELETE) is successful, it will return a JSON with a success message. It will also have a key called 'message' with an endpoint URL as value. Making a GET request to this URL will give the status of the request and response.

Following is an example of a request and its response:

Request

GET

```
https://api-server-host-name/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}
```

Response

```
{
   "request":{
      },
   "response":{
      "node_change_count":-1,
      "errors":[
         ],
      "delete_remote_device":[
         "192.168.34.23"
         ],
      "message":"Device deleted",
      "success":true
   }
}
```

CHAPTER

FOUR

ALERTRULES

4.1 AlertRules - Activate

Activates the alert rule with given id .

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/AlertRules/{id}/
↪activate
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Alert rule id . Mandatory Field

Request Example

```
{
    "data": {}
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

4.2 AlertRules - Create

Create a new alert rule

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/AlertRules
```

Parameter

Field	Label in UI	Type	Description
aggregate	Risk Calculation Function	String	Risk Calculation Function. Accepts values such as "min","max" and "avg". Used for calculating Risk Value of the alert. Mandatory Field
alert_context_template	Template Syntax	String	Specify the Jinja Template syntax for rows that will be displayed in the Incident Data View. Optional Field
assigned_to	Assigned To	String	ID of the user who can re-assign, comment on and view the data of the generated incident. Optional Field
attack_tag	Attack Tag	[String]	List of attack tag IDs to categorize the alert rules. Use MitreAttacks - FetchMitreAttacks to obtain value for this parameter. Optional Field
condition_option	Condition	String	Accepts values such as "greaterthan", "lessthan", "equalsto", "lessequal", "equals", "moreequal" and "notequal". Mandatory Field
condition_value	Condition	int	Can be positive integer or 0. Mandatory Field
delay_interval_minute	Delay Threshold (Minutes)	int	Specify the value of delay interval in minutes to wait for the logs before processing. To set the value, "timestamp_on" parameter value must be "log_ts" in SystemSettingsGeneral API. Accepts values from 1 to 1440 only. Optional Field.
description	Description	String	Description of the alert rule. Optional Field

Continued on next page

Table 2 – continued from previous page

Field	Label in UI	Type	Description
flush_on_trigger	Flush On Trigger	String	Enabling Flush on Trigger activates the next alert rule only by new set of events. Accepts only "on" as value to enable flush on trigger. Optional Field
limit	Limit	int	Number of logs. Minimum value for the field is 1. Mandatory Field
log_source	Log Sources	[String]	List of log sources from where the logs should be collected. Optional Field
manageable_by	Manageable by	[String]	A list of incident user groups ID where users can re-assign, comment on, view data and resolve the generated incidents. Optional Field
metadata	Metadata	[json]	Optional Field. Array of key-value pair objects to define custom metadata for an alert rule. Each object in the array must include the following parameters: **field**: Field for the custom metadata. **value**: Value associated with the given field.
original_data	Alert using original data	boolean	Alert will be generated with encrypted data where Data Privacy Module is enabled. Setting this value as "true" sends request to generate alert with original data. Can be true/false. Optional Field
owner	-	String	ID of the user who owns alert rule. Mandatory Field
query	Query	String	The query for which the alert rule should be fired. Optional Field

Continued on next page

Table 2 – continued from previous page

Field	Label in UI	Type	Description
repos	Repos	[String]	The list of the Repos that you want to monitor for the matching alert condition. Use Repos - FetchRemoteRepos to obtain value for this parameter. Mandatory Field
risk	Risk	String	Risk level of the Alert. Accepts values such as "low", "medium", "high" and "critical". Used for calculating Risk Value of the alert. Mandatory Field
search_interval_minute	Search Interval (Minutes)	int	Specify the custom search interval for retrieving the logs via search in minutes. Optional Field
searchname	Name	String	Name of the alert. It should be a unique valid string. Mandatory Field
throttling_enabled	Alert Throttling	String	Accepts "on" as value to enable Alert Throttling. Can be "on" only. Optional Field
throttling_field	Field	String	Specify a field on the basis of which alert throttling will be applied. Can be positive integer or 0. Mandatory only when the value of throttling_enabled is "on". Optional Field
throttling_time_range	Minutes	int	Specify a time in minutes for which alert will not be dispatched. Mandatory only when the value of the value of throttling_enabled is "on". Optional Field
timerange_day	Day	int	Specify the timerange in Day for which the alert condition is to be matched. Either timerange_day or timerange_hour must be present when timerange_minute is not present in the request. Optional Field

Continued on next page

Table 2 – continued from previous page

Field	Label in UI	Type	Description
timerange_hour	Hour	int	Specify the timerange in Hour for which the alert condition is to be matched. Either timerange_day or timerange_hour must be present when timerange_minute is not present in the request. Optional Field
timerange_minute	Minute	int	Specify the timerange in Minute for which the alert condition is to be matched. Mandatory only when timerange_day and timerange_hour is not present in the request. Optional Field

Request Example

```
{
  "data": {
    "aggregate": "min",
    "alert_context_template": "{% for item in rows %}{{ item.col_ts }}{{item.device_ip}}{{item.
↪source_address}}{%- endfor %}",
    "assigned_to": "5b2a1204d8aaa4136bd32baa",
    "attack_tag": [
      "fa31b91e608e4d840a773d891f3e0a84",
      "bfe6e195e59084a433a6cf3083056b01"
    ],
    "condition_option": "greaterthan",
    "condition_value": 5,
    "delay_interval_minute": 5,
    "description": "Notification of average severity level per device",
    "flush_on_trigger": "on",
    "limit": 25,
    "log_source": [
      "log1",
      "log2"
    ],
    "manageable_by": [
      "5a467b3dd8aaa461c3139038",
      "5a467b3dd8aaa461c3139039"
    ],
    "metadata": [
      {
        "field": "device_ip",
        "value": "127.0.0.1"
```

(continues on next page)

(continued from previous page)

```
            },
            {
                "field": "device_name",
                "value": "localhost"
            }
        ],
        "original_data": "true",
        "owner": "5a466e9dd8aaa4748d3977c7",
        "query": "severity=*|chart avg(severity) by device_ip",
        "repos": [
            "127.0.0.1:5504/_LogPointAlerts",
            "127.0.0.1:5504/_logpoint"
        ],
        "risk": "medium",
        "search_interval_minute": 5,
        "searchname": "Average severity level per device",
        "throttling_enabled": "on",
        "throttling_field": "user",
        "throttling_time_range": 5,
        "timerange_hour": 2
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

4.3 AlertRules - Deactivate

Deactivates the alert rule with given id .

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/AlertRules/{id}/
↪deactivate
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Alert rule id . Mandatory Field

Request Example

```
{
   "data": {}
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

4.4 AlertRules - Edit

Edit alert rule with given id

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/AlertRules/{id}
```

Parameter

Field	Label in UI	Type	Description
aggregate	Risk Calculation Function	String	Risk Calculation Function. Accepts values such as "min","max" and "avg". Used for calculating Risk Value of the alert. Mandatory Field
alert_context_template	Template Syntax	String	Specify the Jinja Template syntax for rows that will be displayed in the Incident Data View. Optional Field
assigned_to	Assigned To	String	ID of the user who can re-assign, comment on and view the data of the generated incident. Optional Field
attack_tag	Attack Tag	[String]	List of attack tag IDs to categorize the alert rules. Use MitreAttacks - FetchMitreAttacks to obtain value for this parameter. Optional Field

Continued on next page

Table 4 – continued from previous page

Field	Label in UI	Type	Description
condition_option	Condition	String	Accepts values such as "greaterthan", "lessthan", "equalsto", "lessequal", "equals", "moreequal" and "notequal". Mandatory Field
condition_value	Condition	int	Can be positive integer or 0. Mandatory Field
delay_interval_minute	Delay Threshold (Minutes)	int	Specify the value of delay interval in minutes to wait for the logs before processing. To set the value, "timestamp_on" parameter value must be "log_ts" in SystemSettingsGeneral API. Accepts values from 1 to 1440 only. Optional Field
description	Description	String	Description of the alert rule. Optional Field
flush_on_trigger	Flush On Trigger	String	Enabling Flush on Trigger activates the next alert rule only by new set of events. Accepts only "on" as value to enable flush on trigger. Optional Field
id	-	String	Alert rule id . Mandatory Field
limit	Limit	int	Number of logs. Minimum value for the field is 1. Mandatory Field
log_source	Log Sources	[String]	List of log sources from where the logs should be collected. Optional Field
manageable_by	Manageable by	[String]	A list of incident user groups ID where users can re-assign, comment on, view data and resolve the generated incidents. Optional Field

Continued on next page

Table 4 – continued from previous page

Field	Label in UI	Type	Description
metadata	Metadata	[json]	Optional Field. Array of key-value pair objects to define custom metadata for an alert rule. Each object in the array must include the following parameters: **field**: Field for the custom metadata. **value**: Value associated with the given field.
original_data	Alert using original data	boolean	Alert will be generated with encrypted data where Data Privacy Module is enabled. Setting this value as "true" sends request to generate alert with original data. Can be true/false. Optional Field
query	Query	String	The query for which the alert rule should be fired. Optional Field
repos	Repos	[String]	The list of the Repos that you want to monitor for the matching alert condition. Mandatory Field
risk	Risk	String	Risk level of the Alert. Accepts values such as "low", "medium", "high" and "critical". Used for calculating Risk Value of the alert. Mandatory Field
search_interval_minute	Search Interval (Minutes)	int	Specify the custom search interval for retrieving the logs via search in minutes. Optional Field
searchname	Name	String	Name of the alert rule. It should be a unique valid string. Mandatory Field
throttling_enabled	Alert Throttling	String	Accepts "on" as value to enable Alert Throttling. Can be "on" only. Optional Field

Continued on next page

Table 4 – continued from previous page

Field	Label in UI	Type	Description
throttling_field	Field	String	Specify a field on the basis of which alert throttling will be applied. Can be positive integer or 0. Mandatory only when the value of throttling_enabled is "on". Optional Field
throttling_time_range	Minutes	int	Specify a time in minutes for which alert will not be dispatched. Mandatory only when the value of the value of throttling_enabled is "on". Optional Field
timerange_day	Day	int	Specify the timerange in Day for which the alert condition is to be matched. Either timerange_day or timerange_hour must be present when timerange_minute is not present in the request. Optional Field
timerange_hour	Hour	int	Specify the timerange in Hour for which the alert condition is to be matched. Either timerange_day or timerange_hour must be present when timerange_minute is not present in the request. Optional Field
timerange_minute	Minute	int	Specify the timerange in Minute for which the alert condition is to be matched. Mandatory only when timerange_day and timerange_hour is not present in the request. Optional Field

Request Example

```
{
   "data": {
      "aggregate": "min",
      "alert_context_template": "{% for item in rows %}{{ item.col_ts }}{{item.device_ip}}{{item.
↪source_address}}{%- endfor %}",
      "assigned_to": "5b2a1204d8aaa4136bd32baa",
      "attack_tag": [
         "fa31b91e608e4d840a773d891f3e0a84",
```

(continues on next page)

(continued from previous page)

```
      "bfe6e195e59084a433a6cf3083056b01"
    ],
    "condition_option": "greaterthan",
    "condition_value": 5,
    "delay_interval_minute": 5,
    "description": "Notification of average severity level per device",
    "flush_on_trigger": "on",
    "limit": 25,
    "log_source": [
      "log1",
      "log2"
    ],
    "manageable_by": [
      "5a467b3dd8aaa461c3139038",
      "5a467b3dd8aaa461c3139039"
    ],
    "metadata": [
      {
        "field": "device_ip",
        "value": "127.0.0.1"
      },
      {
        "field": "device_name",
        "value": "localhost"
      }
    ],
    "original_data": "true",
    "query": "severity=*|chart avg(severity) by device_ip",
    "repos": [
      "127.0.0.1:5504/_LogPointAlerts",
      "127.0.0.1:5504/_logpoint"
    ],
    "risk": "medium",
    "search_interval_minute": 5,
    "searchname": "Average severity level per device",
    "throttling_enabled": "on",
    "throttling_field": "user",
    "throttling_time_range": 5,
    "timerange_minute": 10
  }
}
```

Success Response

```
{
```

(continues on next page)

(continued from previous page)

```
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

4.5 AlertRules - EmailNotification

Setup email notification for an alert rule

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/AlertRules/{id}/
↪EmailNotification
```

Parameter

Field	Label in UI	Type	Description
b64_logo	-	String	Base64 encoded logo image. Only "jpeg" image type upto 160*75 dimension is allowed. Should be a comma separated value containing type of image and base64 encoded value. Mandatory only when the value of logo_enable is "true". Optional Field
dispatch_option	Notification Trigger	String	Describes the notification trigger mechanism. Value can be either "auto" or "manual". Value must be "auto" to automatically trigger the notification and the value must be "manual" to manually trigger the notification. Optional Field
email_emails	Emails	[String]	Accepts a list of email addresses where you want to setup the email notification. Mandatory only when the value of notify_email is "on". Optional Field
email_template	Message	String	Message of the Email. Optional Field

Continued on next page

Table 5 – continued from previous page

Field	Label in UI	Type	Description
email_threshold_option	Threshold	String	Time Unit for email threshold. Can be minute/hour/day. Mandatory only when the value of email_threshold_value is required. Optional Field
email_threshold_value	Threshold	int	Value for email threshold. Can be positive integer. Mandatory only when the value of email_threshold_option is required. Optional Field
id	-	String	Alert rule id . Mandatory Field
link_disable	Disable Search Link	boolean	Value must be "true" to disable the search link in the email or must be "false" to enable the search link in the email. Optional Field
logo_enable	Enable Logo	boolean	Value must be "true" to add a logo or "false" to remove/disable the logo. Optional Field
notify_email	Notify via email	String	Accepts on/off as values to enable/disable email notification for an alert rule. Mandatory Field
subject	Subject	String	Subject of the Email. Optional Field

Request Example

```
{
   "data": {
      "b64_logo": "data:image/jpeg;base64,/9j/4AAQSkZJRgABAQAAAQABAAD/
↪2wBDAAMCAgICAgMCAgIDAwMDBAYEBAQEBAgGBgUGCQgKCgkICQkKDA8MCgsOCwkJDRENDg8QEB
↪2wBDAQMDAwQDBAgEBAgQCwkLEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBA
↪wAARCAAhACIDASIAAhEBAxEB/8QAFwABAQEBAAAAAAAAAAAAAAAAAAAYHCf/
↪EACMQAAEDBAIDAAMAAAAAAAAAAAAEAAgQDBgcRBSESFDETIlH/
↪xAAYAQADAQEAAAAAAAAAAAAAAAAAAAgMBBP/
↪EACARAAICAgIDAQEAAAAAAAAAAAAEDAAIEESExEhNBBVH/2gAMAwEAAhEDEQA/
↪AOqaIozKeTIOLuBoc1M4yvPdKkiLSo0nBvfg55cSd6Aax3wEk6AHaatTc+I7jrVd1wtY2T8Es0WYY2zhFyDcL7dfbM
↪OOhwa0j8RhyvZaTvs+DmfR8On7B/
↪oVWim5VXrK79H+cS2PkMxWhyjqw6mSY1wjLsS+JF0O5WK6GYdSLHiUKWiC97HEk6DQB4dADsuJJWtoi1dPX
↪/9k=",
      "dispatch_option": "auto",
      "email_emails": [
         "rp@gmail.com",
         "sp@gmail.com"
```

(continues on next page)

(continued from previous page)

```
    ],
    "email_template": "This is to notify the user that the user logged more than 5 times.",
    "email_threshold_option": "minute",
    "email_threshold_value": 5,
    "link_disable": "false",
    "logo_enable": "true",
    "notify_email": "on",
    "subject": "The user logged more than 5 times."
  }
}
```

Success Response

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

4.6 AlertRules - FetchMyRules

Fetches all alert rules defined under MyRules.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/AlertRules/
↪MyAlertRules/fetch
```

Parameter

Field	Label in UI	Type	Description
active	-	boolean	Status(active/deactive) of the alert rules to fetch. Setting this value as "true" sends request to generate all active alert rules defined under MyRules section. Can be true/false. Optional Field
log_source	-	[String]	List of log sources. Filters alert rules according to the specified log sources in the list. If at least one log source in the alert rule matches one in the list, it is included in the filtered results. Optional Field.

Request Example

```
{
   "data": {
      "active": "true",
      "log_source": [
         "log1",
         "log2"
      ],
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}/{data_node}"
}
```

4.7 AlertRules - FetchSharedRules

Fetches all alert rules that has been shared.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/AlertRules/
↪SharedAlertRules/fetch
```

Parameter

Field	Label in UI	Type	Description
active	-	boolean	Status(active/deactive) of the alert rules to fetch. Setting this value as "true" sends request to generate all active alert rules defined under SharedRules section. Can be true/false. Optional Field

Continued on next page

Table 7 – continued from previous page

Field	Label in UI	Type	Description
log_source	-	[String]	List of log sources. Filters alert rules according to the specified log sources in the list. If at least one log source in the alert rule matches one in the list, it is included in the filtered results. Optional Field.

Request Example

```
{
    "data": {
        "active": "true",
        "log_source": [
            "log1",
            "log2"
        ],
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}/{data_node}"
}
```

4.8 AlertRules - FetchUsedRules

Fetches all the vendor alert rules that have been used.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/AlertRules/
↪UsedAlertRules/fetch
```

Parameter

Field	Label in UI	Type	Description
active	-	boolean	Status(active/deactive) of the alert rules to fetch. Setting this value as "true" sends request to generate all active alert rules defined under UsedRules section. Can be true/false. Optional Field
log_source	-	[String]	List of log sources. Filters alert rules according to the specified log sources in the list. If at least one log source in the alert rule matches one in the list, it is included in the filtered results. Optional Field.

Request Example

```
{
   "data": {
      "active": "true",
      "log_source": [
         "log1",
         "log2"
      ],
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}/{data_node}"
}
```

4.9 AlertRules - FetchUsedSharedRules

Fetches the alert rules that were shared by users and are currently being used in the given Logpoint.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/AlertRules/
↪UsedSharedAlertRules/fetch
```

Parameter

Field	Label in UI	Type	Description
active	-	boolean	Status(active/deactive) of the alert rules to fetch. Setting this value as "true" sends request to generate all active alert rules defined under UsedSharedRules section. Can be true/false. Optional Field
log_source	-	[String]	List of log sources. Filters alert rules according to the specified log sources in the list. If at least one log source in the alert rule matches one in the list, it is included in the filtered results. Optional Field.

Request Example

```
{
   "data": {
      "active": "true",
      "log_source": [
         "log1",
         "log2"
      ],
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}/{data_node}"
}
```

4.10 AlertRules - FetchVendorRules

Fetches all alert rules provided by the vendor.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/AlertRules/
↪VendorAlertRules/fetch
```

Parameter

Field	Label in UI	Type	Description
log_source	-	[String]	List of log sources. Filters alert rules according to the specified log sources in the list. If at least one log source in the alert rule matches one in the list, it is included in the filtered results. Optional Field.

Request Example

```
{
   "data": {
      "log_source": [
         "log1",
         "log2"
      ],
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}/{data_node}"
}
```

4.11 AlertRules - HTTPNotification

Setup HTTP notification for an alert rule.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/AlertRules/{id}/
↪HTTPNotification
```

Parameter

Field	Label in UI	Type	Description
dispatch_option	Notification Trigger	String	Describes the notification trigger mechanism. Value can be either "auto" or "manual". Value must be "auto" to automatically trigger the notification and the value must be "manual" to manually trigger the notification. . Optional Field.
http_body		String	Provides a template for the body of the HTTP notification in the String format. Provide the http_body only when http_request_type is POST, PUT, and PATCH. Optional Field.
http_header	Headers	json	To define http_header, you must provide the following parameters. auth_type : Value can be "basic_auth", "api_token", "bearer_token". Mandatory auth_key : Authorization Key. Mandatory only when auth_type is set as basic_auth, api_token or bearer_token. auth_value : Authorization Value. Mandatory only when auth_type is set as api_token. auth_pass : Authorization Password. Mandatory only when auth_type is set as basic_auth. Optional Field.
http_querystring	Query String	String	Query string. Mandatory only when the value of notify_http is "on". Optional Field.
http_request_type	Request Type	String	Request type of HTTP. Can be GET/POST/PUT/DELETE/PATCH/HEAD. Mandatory only when the value of notify_http is "on". Optional Field.
http_threshold_option	Threshold	String	Time Unit for http threshold. Can be minute/hour/day. Mandatory only when the value of http_threshold_value is required. Optional Field.

Continued on next page

Table 11 – continued from previous page

Field	Label in UI	Type	Description
http_threshold_value	Threshold	int	Value for http threshold. Can be positive integer. Mandatory only when the value of http_threshold_option is required. Optional Field.
http_url	Base URL	String	Contains URL to send HTTP notification. Mandatory only when the value of notify_http is "on". Optional Field.
id	-	String	Alert rule id . Mandatory Field.
notify_http	Notify via HTTP	String	Accepts on/off as values to enable/disable http notification for an alert rule. Mandatory Field.
protocol	Protocol	String	Protocol to send the HTTP Notification. Can be HTTP/HTTPS. By default protocol will be set to HTTP in logpoint if value of notify_http is "on" and no protocol parameter is present in request. Optional Field.

Request Example

```
{
  "data": {
    "http_body": "{\"title\": \"{{alert_name}}\", \"description\": \"{{description}}\", \"risk\": \"{{risk}}\", \"dispatch_option\": \"auto\", \"query\": \"{{ extra_info.query }}\"}",
    "http_header": {
      "auth_key": "key1",
      "auth_pass": "pwd1",
      "auth_type": "basic_auth"
    },
    "http_querystring": "user='admin'&count=rows_count",
    "http_request_type": "POST",
    "http_threshold_option": "minute",
    "http_threshold_value": 5,
    "http_url": "http://www.test.com/try",
    "notify_http": "on"
  }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

4.12 AlertRules - Install

Install a given alertrule pak file

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/AlertRules/install
```

Parameter

Field	Label in UI	Type	Description
file_location	-	String	Location of the file to install. Can be either 'private' or 'public'. Mandatory Field
file_name	Alert Rules	String	Name of the pak file for AlertRules. Mandatory Field
owner	-	String	ID of the user who owns alert rule. Mandatory Field

Request Example

```
{
   "data": {
      "file_location": "private",
      "file_name": "alert1.pak",
      "owner": "5a466e9dd8aaa4748d3977c7"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

4.13 AlertRules - ListPrivateUploads

List all the pak files that contains alert rules in private storage

GET

```
https://api-server-host-name/configapi/{pool_UUID}/AlertRules/list
```

Success Response

```
[
   "test.pak"
]
```

4.14 AlertRules - ListPublicUploads

List all the pak files that contains alert rules in public storage

GET

```
https://api-server-host-name/configapi/AlertRules/list
```

Success Response

```
[
   "test.pak"
]
```

4.15 AlertRules - SMSNotification

Setup SMS notification for an alert rule.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/AlertRules/{id}/
↪SMSNotification
```

Parameter

Field	Label in UI	Type	Description
dispatch_option	Notification Trigger	String	Describes how a notification is triggered. Value can be the default "auto", or "manual". "Auto" automatically triggers a notification and "manual" requires a user to do it. Optional Field.
id	-	String	Alert rule id. Mandatory Field.
notify_sms	Notify via SMS	String	Accepts on/off as values to enable/disable sms notification for an alert rule. Mandatory Field.
sms_body	Body	String	SMS notification message. Optional Field.
sms_password	Password	String	sms_server password. Mandatory only when the value of notify_sms is "on". Optional Field.
sms_port	Port	int	Port number of sms_server. Mandatory only when the value of notify_sms is "on". Optional Field.
sms_receivers	Receivers	[String]	List of receiver phone numbers. The receivers' numbers must be between 3 and 15 numerical digits. Mandatory only when the value of notify_sms is "on". Optional Field.
sms_sender	Sender ID	String	Sender ID for the sms_server. Mandatory only when the value of notify_sms is "on". Optional Field.
sms_server	SMSC Server	String	Destination server address. Mandatory only when the value of notify_sms is "on". Optional Field.
sms_threshold_option	Threshold	String	Time Unit for sms threshold. Can be minute/hour/day. Mandatory only when the value of sms_threshold_value is required. Optional Field.

Continued on next page

Table 13 – continued from previous page

Field	Label in UI	Type	Description
sms_threshold_value	Threshold	int	Value for sms threshold. Can be a positive integer. Mandatory only when the value of sms_threshold_option is present in the request. Optional Field.
sms_username	Username	String	Username for the sms_server. Mandatory only when the value of notify_sms is "on". Optional Field.

Request Example

```
{
   "data": {
      "dispatch_option": "auto",
      "notify_sms": "on",
      "sms_body": "New alert dispatched",
      "sms_password": "password1",
      "sms_port": 2775,
      "sms_receivers": [
         "+998939893",
         "5110521"
      ],
      "sms_sender": "SH-LPO",
      "sms_server": "127.0.0.1",
      "sms_threshold_option": "minute",
      "sms_threshold_value": 5,
      "sms_username": "johnwatson"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

4.16 AlertRules - SNMPNotification

Setup SNMP notification for an alert rule

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/AlertRules/{id}/
↪SNMPNotification
```

Parameter

Field	Label in UI	Type	Description
dispatch_option	Notification Trigger	String	Describes the notification trigger mechanism. Value can be either "auto" or "manual". Value must be "auto" to automatically trigger the notification and the value must be "manual" to manually trigger the notification. . Optional Field
id	-	String	Alert rule id . Mandatory Field
notify_snmp	Notify via SNMP Traps	String	Accepts on/off as values to enable/disable snmp notification for an alert rule. Mandatory Field
snmp_agent	Agent	String	Name of the agent that sends SNMP trap. Mandatory only when the value of snmp_version is SNMPv2c. Optional Field
snmp_authorization_key	Authorization Key	String	Authorization Key for SNMPv3. Mandatory only when the value of snmp_version is SNMPv3. Optional Field
snmp_community_string	Community String	String	Passphrase in the Community String. Mandatory only when the value of snmp_version is SNMPv2c. Optional Field
snmp_ip	IP	String	IP address of trap receiver. Mandatory only when the value of notify_snmp is "on". Optional Field
snmp_message	Message	String	OID's corresponding value in the Message. Optional Field

Continued on next page

Table 14 – continued from previous page

Field	Label in UI	Type	Description
snmp_oid	OID	String	Valid SNMP trap or Enterprise specific OID [Object Identifier] to the corresponding alert in the dotted decimal format. Make sure not to use the OID with leading dot while sending SNMP traps notifications in alerts. Mandatory only when the value of notify_ssh is "on". Optional Field
snmp_port	Port	int	Port number of trap receiver. Mandatory only when the value of notify_snmp is "on". Optional Field
snmp_private_key	Private Key	String	Private Key for SNMPv3. Mandatory only when the value of snmp_version is SNMPv3. Optional Field
snmp_threshold_option	Threshold	String	Time Unit for snmp threshold. Can be minute/hour/day. Mandatory only when the value of snmp_threshold_value is required. Optional Field
snmp_threshold_value	Threshold	int	Value for snmp threshold. Can be positive integer. Mandatory only when the value of snmp_threshold_option is required. Optional Field
snmp_username	Username	String	Username for SNMPv3. Mandatory only when the value of snmp_version is SNMPv3. Optional Field
snmp_version	SNMP Version	String	Version can be SNMPv2c or SNMPv3. Mandatory only when the value of notify_snmp is "on". Optional Field

Request Example

```
{
   "data": {
      "dispatch_option": "auto",
      "notify_snmp": "on",
```

(continues on next page)

(continued from previous page)

```
        "snmp_agent": "192.168.3.12",
        "snmp_community_string": "public",
        "snmp_ip": "10.45.9.20",
        "snmp_message": "Alert rule was fired.",
        "snmp_oid": "1.3.6.1.4.1.8072.1.2.1.1.5.0.1.2.05",
        "snmp_port": 192,
        "snmp_threshold_enabled": "on",
        "snmp_threshold_option": "minute",
        "snmp_threshold_value": 5,
        "snmp_version": "SNMPv2c"
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

4.17 AlertRules - SSHNotification

Setup SSH notification for an alert rule.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/AlertRules/{id}/
↪SSHNotification
```

Parameter

Field	Label in UI	Type	Description
dispatch_option	Notification Trigger	String	Describes the notification trigger mechanism. Value can be either "auto" or "manual". Value must be "auto" to automatically trigger the notification and the value must be "manual" to manually trigger the notification. . Optional Field
id	-	String	Alert rule id . Mandatory Field
notify_ssh	Notify via SSH	String	Accepts on/off as values to enable/disable ssh notification for an alert rule. Mandatory Field

Continued on next page

Table 15 – continued from previous page

Field	Label in UI	Type	Description
ssh_auth_password	Password	String	Password. Mandatory only when the value of ssh_auth_type is "password". Optional Field
ssh_auth_type	Authentication	String	Specify the auth type which can be "password" or "certificate". Mandatory only when the value of notify_ssh is "on". Optional Field
ssh_cert_type	Certificate Type	String	Type of Certificate. Use ssh_cert_type when ssh_auth_type is certificate. Values can be system_cert for system certificate and user_cert for user certificate. Optional Field
ssh_command	Command	String	Command you want to execute when the alert rule is fired. Make sure that the command is a valid bash command and is executable. Mandatory only when the value of notify_ssh is "on". Optional Field
ssh_port	Port	int	Port number. Mandatory only when the value of notify_ssh is "on". Optional Field
ssh_server	Server	String	Destination server address. Mandatory only when the value of notify_ssh is "on". Optional Field
ssh_threshold_option	Threshold	String	Time Unit for ssh threshold. Can be minute/hour/day. Mandatory only when the value of ssh_threshold_value is required. Optional Field
ssh_threshold_value	Threshold	int	Value for ssh threshold. Can be positive integer. Mandatory only when the value of ssh_threshold_option is required. Optional Field
ssh_username	Username	String	Username for the user in destination server. Mandatory only when the value of notify_ssh is "on". Optional Field

Request Example

```
{
   "data": {
      "dispatch_option": "auto",
      "notify_ssh": "on",
      "ssh_auth_password": "password1",
      "ssh_auth_type": "password",
      "ssh_command": "command1",
      "ssh_port": 22,
      "ssh_server": "10.45.9.18",
      "ssh_threshold_option": "minute",
      "ssh_threshold_value": 5,
      "ssh_username": "username1"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

4.18 AlertRules - ShareWithUsers

Shares the alert rule by given id with specified usergroups or users with specific permissions.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/AlertRules/{id}/share
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Alert rule id . Mandatory Field

Continued on next page

Table 16 – continued from previous page

Field	Label in UI	Type	Description
rbac_config	-	[json]	Alert sharing config using RBAC. Either it can be empty list or following parameters should be provided to define rbac_config. group_id : Id of usergroup. Mandatory field. group_permission : Permission at the group level. Optional field. Can be either "READ", "EDIT" or "FULL". Either group_permission or user_permissions must be present in the request. If present, user_permissions should not be present in request and this permission applies to all users in that group. user_permissions : List of user permissions. Either group_permission or user_permissions must be present in the request. If present, should not be empty list. Must have at least one user permission object. To define user_permissions following parameters should be used. user_id : Id of user for which permission is to be assigned. Mandatory field. permission : Can be either "READ", "EDIT" or "FULL". Mandatory field. . Mandatory Field

Request Example

```
{
   "data": {
      "rbac_config": [
         {
            "group_id": "60616651b8a4470f71510082",
            "group_permission": "READ"
         },
         {
```

(continues on next page)

(continued from previous page)

```
                "group_id": "605c56cacec4f90f9786cc87",
                "user_permissions": [
                    {
                        "permission": "EDIT",
                        "user_id": "605c56f36253bcd9fb1d1d67"
                    },
                    {
                        "permission": "FULL",
                        "user_id": "60640a538501f571ab422732"
                    }
                ]
            }
        ]
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

4.19 AlertRules - SyslogNotification

Setup SNMP notification for an alert rule

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/AlertRules/{id}/
↪SyslogNotification
```

Parameter

Field	Label in UI	Type	Description
dispatch_option	Notification Trigger	String	Describes the notification trigger mechanism. Value can be either "auto" or "manual". Value must be "auto" to automatically trigger the notification and the value must be "manual" to manually trigger the notification. . Optional Field

Continued on next page

Table 17 – continued from previous page

Field	Label in UI	Type	Description
facility	Facility	int	Facility of the Syslog Notification. Values can be from 0 to 23 indicating different levels of facility of the Syslog Notification. Optional Field
id	-	String	Alert rule id . Mandatory Field
message	Message	String	Free-form message that provides information about the event. Optional Field
notify_syslog	Notify via Syslog	String	Accepts on/off as values to enable/disable syslog notification for an alert rule. Mandatory Field
port	Port	int	Port number of the remote syslog server where the notification should be sent. Mandatory only when the value of notify_syslog is "on". Optional Field
protocol	-	String	Protocol to send the Syslog Notification. Can be UDP/TCP. Mandatory only when the value of notify_syslog is "on". Optional Field
server	Server	String	Server address of the remote syslog server where the notification should be sent. Mandatory only when the value of notify_syslog is "on". Optional Field
severity	Severity	int	Severity and Facility of the Syslog Notification. Values can be from 0 to 7 indicating different levels of severity of the Syslog Notification. Mandatory only when the value of notify_syslog is "on". Optional Field

Continued on next page

Table 17 – continued from previous page

Field	Label in UI	Type	Description
split_rows	-	boolean	Can be true/false. Select the Send each new line as separate syslognotification option to generate one syslogmessage for each log message in the search result. If this option is not selected, all messages within the chosen time range of the incident are compressed into one syslog message in the search result. Optional Field
threshold_option	Threshold	String	Time Unit for syslog threshold. Can be minute/hour/day. Mandatory only when the value of threshold_value is required. Optional Field
threshold_value	Threshold	int	Value for syslog threshold. Can be positive integer or 0. Mandatory only when the value of threshold_option is required. Optional Field

Request Example

```
{
   "data": {
      "dispatch_option": "auto",
      "facility": 9,
      "message": "The user logged more than 5 times.",
      "notify_syslog": "on",
      "port": 192,
      "protocol": "UDP",
      "server": "10.45.9.20",
      "severity": 4,
      "split_rows": "true",
      "threshold_option": "minute",
      "threshold_value": 5
   }
}
```

Success Response

```
{
```

(continues on next page)

(continued from previous page)

```
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

4.20 AlertRules - TransferOwnership

Transfer ownership of the alert rule to another user.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/AlertRules/{id}/
↪transferOwnership
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Alert rule id . Mandatory Field
userid	-	String	Transfer ownership of the alert rule with given User id. Mandatory Field

Request Example

```
{
    "data": {
        "userid": "574fceedd8aaa40740736302"
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

4.21 AlertRules - Trash

Deletes the alert rule with given id .

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/AlertRules/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Alert rule id . Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

4.22 AlertRules - TrashPrivateUploads

Delete the file with given name from private storage

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/AlertRules/{file_name}
```

Parameter

Field	Label in UI	Type	Description
file_name		String	Name of the file to be deleted. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "Alert1.pak successfully deleted"
}
```

4.23 AlertRules - TrashPublicUploads

Delete the file with given name from public storage

DELETE

```
https://api-server-host-name/configapi/AlertRules/{file_name}
```

Parameter

Field	Label in UI	Type	Description
file_name		String	Name of the file to be deleted. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "Alert1.pak successfully deleted"
}
```

4.24 AlertRules - UnshareWithUsers

Unshares the alert rule with given id from all users within the pool.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/AlertRules/{id}/
↪unshare
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Alert rule id . Mandatory Field

Request Example

```
{
   "data": {}
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

4.25 AlertRules - Upload

Upload pak files that contains alert rules to private storage. This upload should be used for alert rules only.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/AlertRules/upload
```

Header

Field	Label in UI	Description
file_name		Name of the file to be uploaded.
Content-Type		application/octet-stream
replace_existing		Set the value of this parameter as 'true' to replace the existing file with the same name with the new file. Default value is 'false'. Value can be 'true' or 'false'. Optional field

Parameter

Field	Label in UI	Type	Description
file	-	[Object]	(pak) to be uploaded. Mandatory Field

Success Response

```
{
  "status": "Success",
  "message": "Alert1.pak successfully uploaded in private storage. "
}
```

4.26 AlertRules - UploadPublic

Upload pak files that contains alert rules to to public storage. This upload should be used for alert rules only.

POST

```
https://api-server-host-name/configapi/AlertRules/publicupload
```

Header

Field	Label in UI	Description
file_name		Name of the file to be uploaded.
Content-Type		application/octet-stream
replace_existing		Set the value of this parameter as 'true' to replace the existing file with the same name with the new file. Default value is 'false'. Value can be 'true' or 'false'. Optional field

Parameter

Field	Label in UI	Type	Description
file	-	[Object]	(pak) to be uploaded. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "Alert1.pak successfully uploaded in public storage."
}
```

4.27 AlertRules - UseAlertRules

Use the alert rules shared by other LogPoint users or the vendor alert rules.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/AlertRules/{id}/
↪useAlertRules
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Alert rule id . Mandatory Field
owner	-	String	ID of the user who will use the given alert rule. Mandatory Field

Request Example

```
{
   "data": {
      "owner": "5a466e9dd8aaa4748d3977c7"
   }
```

(continues on next page)

(continued from previous page)

```
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

4.28 AlertRules - UseVendorRules

Use the alert rules provided by your vendor.

DEPRECATED ! *Will be removed in future version. Use <b>AlertRules - UseAlertRules</b> API instead.*

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/AlertRules/{id}/
↪useVendorRules
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Alert rule id . Mandatory Field
owner	-	String	ID of the user who owns alert rule. Mandatory Field

Request Example

```
{
   "data": {
      "owner": "5a466e9dd8aaa4748d3977c7"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

FIVE

BACKUPANDRESTORE

5.1 BackupAndRestore - BackupNow

Adds a backup of DB configuration at the current time.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/BackupAndRestore/
↪backupnow
```

Parameter

Field	Label in UI	Type	Description
report_backup	Report Backup	boolean	Create a backup for the generated report files. Value can be set as “true” or “false”. Mandatory Field

Request Example

```
{
   "data": {
      "report_backup": "true"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

5.2 BackupAndRestore - CreateConfigBackup

Back up the configuration details of Fabric-enabled LogPoint and all of its collectors/fetchers.

POST

https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/BackupAndRestore

Parameter

Field	Label in UI	Type	Description
authorized_keys	Public Key	String	Part of Encryption key of the li-admin . Obtain the value of this parameter using Certificate - List API. Optional Field
conf_scheduled_retention	Backup Retention	int	Retention period for the configuration backup in days. Value must be >=1. Mandatory only when "schedule_configuration_backup" is set as "on". Optional Field
conf_scheduled_utc_hour	Backup Run Hour	int	Scheduled time for configuration backup in UTC hour. Mandatory only when "schedule_configuration_backup" is set as "on". Optional Field
report_backup	Report Backup	String	Create a backup for the generated report files. Value can be "on" or "off". Set the value as "on" only when you want to back up the configuration immediately. Optional Field
schedule	Interval	String	Interval for the configuration backup. Takes values as daily/weekly/monthly. Mandatory only when "schedule_configuration_backup" is set as "on". Optional Field
schedule_configuration_backup	Schedule Backup	String	Value can be set as "on" or "off". Set the value as "on" when you want to schedule a backup of your configuration. Mandatory Field

Continued on next page

Table 2 – continued from previous page

Field	Label in UI	Type	Description
weekday	-	String	Values can be Sunday, Monday, Tuesday, Wednesday, Thursday, Friday or Saturday to schedule a configuration backup in certain days of a week. Mandatory only if the schedule is set to weekly. Optional Field

Request Example

```
{
  "data": {
    "authorized_keys": "asdfgh",
    "conf_scheduled_retention": 30,
    "conf_scheduled_utc_hour": 0,
    "report_backup": "on",
    "schedule": "weekly",
    "schedule_configuration_backup": "on",
    "weekday": "sunday"
  }
}
```

Success Response

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

5.3 BackupAndRestore - CreateLogsChecksumBackup

Back up the logs, index of the logs and the checksum of the logs of the Fabric-enabled LogPoint.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/BackupAndRestore/
↪logchecksumbackup
```

Parameter

Field	Label in UI	Type	Description
all_time	All Days	String	Backs up all the logs till date. The all_time parameter or the oldest_time parameter is required only when the value of "schedule_log_backup" is "on". Value of the all_time parameter can be "on" or "off". Optional Field
authorized_keys	Public Key	String	Part of Encryption key. Obtain the value of this parameter using Certificate - List API. Optional Field
backup_repos	Repos to Backup	String	Comma separated repo ids or empty. Mandatory if schedule_log_backup is "on". Obtain the value of the required Repo id using Repos - List API. Optional Field
full_backup	Full Backup	String	Backs up logs and checksum of the desired repos in desired time. Value can be set as "on" or "off". If the value of full_backup is set as "on", "scheduled_log_backup" will also be "on" by default. For the value to be "off", both "schedule_log_backup" and "full_backup" must be "off". Optional Field
oldest_time	-	String	Backs up the logs from the given time period. The all_time parameter or the oldest_time parameter is required only when the value of "schedule_log_backup" is "on". Value of the oldest_time parameter must in dd/mm/yyyy format. Optional Field

Continued on next page

Table 3 – continued from previous page

Field	Label in UI	Type	Description
schedule_log_backup	Schedule Backup	String	Backs up logs and checksum of the desired repos in desired time. Value can be set as "on" or "off". For the value to be "off", both "schedule_log_backup" and "full_backup" must be "off". Optional Field
scheduled_retention	Backup Retention	int	integer greater than 0. Should be provided only if schedule_log_backup is 'on'.Retention period for the scheduled backup of Logs Checksum in days. Value must be an integer >=1. Mandatory only when the value of "schedule_log_backup" is set to "on". Optional Field
scheduled_utc_hour	Backup Run Hour	int	Time in UTC hour, from when the backup is started. Integer [0-23]. Mandatory if either 'full_backup' is "on" or 'schedule_log_backup' is "on". Optional Field

Request Example

```
{
   "data": {
      "all_time": "on",
      "authorized_keys": "asdfgh",
      "backup_repos": "547c04fbd8aaa47389671bb2,547c04fbd8aaa47389671bb3",
      "full_backup": "on",
      "oldest_time": "11/11/2017",
      "schedule_log_backup": "off",
      "scheduled_retention": 30,
      "scheduled_utc_hour": 0
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

5.4 BackupAndRestore - Get

Fetches any backup data with given ID.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/BackupAndRestore/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing back up data id .

Success Response

```
{
    "_permission": true,
    "backupdate": "2018-04-18-00-00-00",
    "created_date": "2018/04/18 04:28:19",
    "filename": "logs_2018-04-18.backup",
    "id": "0cafc41559b591b304364e5b9a00d7ed",
    "name": "_logpoint",
    "size": 18160,
    "type": "logs"
}
```

5.5 BackupAndRestore - List

Lists all backup data.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/BackupAndRestore
```

Success Response

```
[
    {
        "_permission": true,
        "backupdate": "2018-04-18-00-00-00",
        "created_date": "2018/04/18 04:28:19",
        "filename": "logs_2018-04-18.backup",
        "id": "0cafc41559b591b304364e5b9a00d7ed",
        "name": "_logpoint",
```

(continues on next page)

(continued from previous page)

```
        "size": 18160,
        "type": "logs"
    },
    {
        "_permission": true,
        "backupdate": "2018-04-13-00-00-00",
        "created_date": "2018/04/17 10:17:52",
        "filename": "logs_2018-04-13.backup",
        "id": "34121959c00fbbc3061ad3921f7a7d7d",
        "name": "_logpoint",
        "size": 8830,
        "type": "logs"
    }
]
```

5.6 BackupAndRestore - ListSettings

Lists the backup and restore settings.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/BackupAndRestore/
↪settings
```

Success Response

```
[
    {
        "authorized_keys": "",
        "backup_repos": [],
        "conf_scheduled_retention": 365,
        "conf_scheduled_utc_hour": 0,
        "from_ts": "",
        "id": "5ac6ef2ed8aaa47316027a3f",
        "schedule": "Monthly",
        "schedule_configuration_backup": "off",
        "schedule_log_backup": "off",
        "scheduled_retention": 365,
        "scheduled_utc_hour": 2,
        "weekday": ""
    }
]
```

5.7 BackupAndRestore - LogChecksumBackupNow

Back up the logs, index of the logs and the checksum of the logs of the Fabric-enabled LogPoint at current time.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/BackupAndRestore/
↪logchecksumbackupnow
```

Request Example

```
{
    "data": {}
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

5.8 BackupAndRestore - RefreshList

Updates the list of backup schedule.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/BackupAndRestore/
↪refreshlist
```

Request Example

```
{
    "data": {}
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

5.9 BackupAndRestore - Restore

Restores the backup data.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/BackupAndRestore/
↪{id}/restore
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing back up data id . Mandatory Field

Request Example

```
{
   "data": {}
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

5.10 BackupAndRestore - Trash

Deletes any backup data with given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/BackupAndRestore/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing back up data id . Mandatory Field

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

SIX

CERTIFICATE

6.1 Certificate - FetchUserSSHCertificate

Fetches the SSH certificate of given user.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Certificate/
↪SSHUserCertificate/fetch
```

Parameter

Field	Label in UI	Type	Description
user_id	-	String	ID of the user whose SSH certificate you want to fetch. Mandatory Field

Request Example

```
{
   "data": {
      "user_id": "5a466e9dd8aaa4748d3977c7"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}/{data_node}"
}
```

6.2 Certificate - List

Lists the authorization certificate for SCP.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Certificate
```

Success Response

```
[
   {
      "public_key": "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQC/
↪iRoSiSgYtHCZnFbA1qo1K4GzNAYAKBoofiN6RBsMX18w4EMjc+1EKVYs1Upw0tsDqreLAMA73yU+koSwbz5Jiw
↪"
   }
]
```

6.3 Certificate - ListSystemSSHCertificate

Lists the SSH certificate of given system.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Certificate/
↪SSHSystemCertificate
```

Success Response

```
[
   {
      "certificate": "ssh-rsa ACAAS3NzaC1xb2EAAAADAQABAAAAgQCp75/
↪8l42sqTAGJmvpYh0A36JBbWclkAX3p9h9lklSle1onmva+VURzYPSzcyfQQLFk+bvsVFQwKbX/
↪f4IbCR/5WRTeqPagsm+57nEXid7xehrb+patdJEmegk5/DmWpw5ZqIOi5kO8/
↪EqFajTlJ+3PquZrxm5EnE4UCdl/pR/gm=="
   }
]
```

CHAPTER

SEVEN

CHARSETS

7.1 Charsets - ListCharsets

List the available charsets

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Charsets
```

Success Response

```
[
    {
        "charsets": [
            "ascii",
            "big5",
            "utf_8",
            "utf_8_sig"
        ]
    }
]
```

CHAPTER

EIGHT

DEVICEGROUPS

8.1 DeviceGroups - Create

Adds a new device group.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/DeviceGroups
```

Parameter

Field	Label in UI	Type	Description
description	Description	String	Description for the device group. Mandatory Field
devices	Devices in this group	[String]	List of device id(s) you want to associate with the device group. Optional Field
name	Name	String	A unique valid string to define the Name of the device group. Mandatory Field

Request Example

```
{
   "data": {
      "description": "CreatedfromZookeper",
      "devices": [
         "5759080fd8aaa41bfef54884"
      ],
      "name": "testgroup1"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

8.2 DeviceGroups - Edit

Edits a device group with given id .

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/DeviceGroups/{id}
```

Parameter

Field	Label in UI	Type	Description
description	Description	String	Description for the device group. Mandatory Field
devices	Devices in this group	[String]	List of device id(s) that you want to associate with the device group. Optional Field
id	-	String	Existing device group id . Mandatory Field
name	Name	String	A unique valid string to define the Name of the device group. Mandatory Field

Request Example

```
{
   "data": {
      "description": "CreatedfromZookeper",
      "devices": [
         "5759080fd8aaa41bfef54884"
      ],
      "name": "testgroup1"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
```

(continues on next page)

(continued from previous page)

```
}
```

8.3 DeviceGroups - Get

Fetches a device group with given id .

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/DeviceGroups/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing device group id .

Success Response

```
{
   "description": "CreatedfromZookeper",
   "devices": [
      "5759080fd8aaa41bfef54884"
   ],
   "id": "574fb123d8aaa4625bfe2d23",
   "name": "testgroup1"
}
```

8.4 DeviceGroups - List

Lists all device groups in the Fabric-enabled LogPoint.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/DeviceGroups
```

Success Response

```
[
   {
      "description": "CreatedfromZookeper",
      "devices": [
         "5759080fd8aaa41bfef54884"
      ],
```

(continues on next page)

(continued from previous page)

```
        "id": "574fb123d8aaa4625bfe2d23",
        "name": "testgroup1"
    }
]
```

8.5 DeviceGroups - Trash

Deletes device group with given id .

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/DeviceGroups/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing device group id . Mandatory Field

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

NINE

DEVICES

9.1 Devices - AddIgnoredIPs

Adds devices to the ignored IP list.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Devices/ignoredips
```

Parameter

Field	Label in UI	Type	Description
ip	-	String	IP address that should be ignored from the list of DetectBlockedIps. Execute Devices - ListBlockedIps API to obtain blocked IP addresses. Mandatory Field

Request Example

```
{
   "data": {
      "ip": "192.168.1.2"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

9.2 Devices - Attach

Attaches devices on behalf of the collector LogPoint from the main LogPoint in a Distributed LogPoint setup.

DEPRECATED ! *Will be removed in future version. Use the distributed_collector parameter of the Devices - Create or Devices - Edit API to attach Distributed collectors.*

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Devices/{id}/attach
```

Parameter

Field	Label in UI	Type	Description
distributed_collector	Distributed Collector	String	Existing Distributed collector id. Obtain the value of the required Distributed collector id using DistributedCollector - List API. . Mandatory Field
id	-	String	Existing Device id. Obtain the value of the required Device id using Devices - List API. Mandatory Field

Request Example

```
{
   "data": {
      "distributed_collector": "574fda0bd8aaa4073b9473d8"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

9.3 Devices - Create

Creates a new device in a Fabric-enabled LogPoint.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Devices
```

Parameter

Field	Label in UI	Type	Description
availability	Availability	String	A string value which could be Minimal, Minor, Major, Critical that defines the availability of the device. Mandatory Field
confidentiality	Confidentiality	String	A string value which could be Minimal, Minor, Major, Critical that defines the confidentiality of the device. Mandatory Field
devicegroup	Device Groups	[String]	List of ID of the existing Device Group where you want to create the device. Use DeviceGroup - List API to obtain the value of the required Device group id. Optional Field
distributed_collector	Distributed Collectors	[String]	List of ID of Distributed Collectors. Use DistributedCollectors - List API to obtain the value of the required Distributed Collectors id. Optional Field
integrity	Integrity	String	A string value which could be Minimal, Minor, Major, Critical that defines the integrity of the device. Mandatory Field
ip	Device address(es)	[String]	Can have valid IP address(es), CIDR address(es), hostname(s) or combination of these as values. Mandatory Field
logpolicy	Log Collection Policy	[String]	List of ID of Log Collection Policies. Use LogCollectionPolicies - List API to obtain the value of the required Log Collection Polices id. Optional Field
name	Name	String	Device name . Mandatory Field

Continued on next page

Table 3 – continued from previous page

Field	Label in UI	Type	Description
timezone	Time Zone	String	An optional string value that specifies the given timezones by logpoint. Obtain the value of the available timezones using Timezone - List API. Optional Field

Request Example

```
{
   "data": {
      "availability": "Minimal",
      "confidentiality": "Minimal",
      "devicegroup": [
         "574fb123d8aaa4625bfe2d23"
      ],
      "distributed_collector": [
         "5db02cbcd8aaa42fddb6f72f"
      ],
      "integrity": "Minimal",
      "ip": [
         "192.168.1.2",
         "google.com"
      ],
      "logpolicy": [
         "5d88c559d8aaa42d8c4bfc41"
      ],
      "name": "device1",
      "timezone": "Asia/Kathmandu"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

9.4 Devices - Detach

Detaches devices on behalf of the collector LogPoint from the main LogPoint in the Distributed LogPoint setup.

DEPRECATED ! *Will be removed in future version. Use the distributed_collector parameter of the Devices - Edit API to detach Distributed collectors.*

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Devices/{id}/detach
```

Parameter

Field	Label in UI	Type	Description
distributed_collector	Distributed Collector	String	Existing Distributed collector id. Obtain the value of the required Distributed collector id using DistributedCollector - List API. . Mandatory Field
id	-	String	Existing Device id. Obtain the value of the required Device id using Devices - List API. Mandatory Field

Request Example

```
{
   "data": {
      "distributed_collector": "574fda0bd8aaa4073b9473d8"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

9.5 Devices - Edit

Edits the device settings with given ID.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Devices/{id}
```

Parameter

Field	Label in UI	Type	Description
availability	Availability	String	A string value which could be Minimal, Minor, Major, Critical that defines the availability of the device. Mandatory Field
confidentiality	Confidentiality	String	A string value which could be Minimal, Minor, Major, Critical that defines the confidentiality of the device. Mandatory Field
devicegroup	Device Groups	[String]	List of ID of the existing Device Group where you want to create the device. Use DeviceGroup - List API to obtain the value of the required Device group id. Optional Field
distributed_collector	Distributed Collectors	[String]	List of ID of Distributed Collectors. Use DistributedCollectors - List API to obtain the value of the required Distributed Collectors id. Optional Field
id	-	String	Existing Device id . Obtain the value of the required Device id using Devices - List API. Mandatory Field
integrity	Integrity	String	A string value which could be Minimal, Minor, Major, Critical that defines the integrity of the device. Mandatory Field
ip	Device address(es)	[String]	Can have valid IP address(es), CIDR address(es), hostname(s) or combination of these as values. Mandatory Field
logpolicy	Log Collection Policy	[String]	List of ID of Log Collection Policies. Use LogCollectionPolicies - List API to obtain the value of the required Log Collection Polices id. Optional Field
name	Name	String	Device name . Mandatory Field

Continued on next page

Table 5 – continued from previous page

Field	Label in UI	Type	Description
timezone	Time Zone	String	An optional string value that specifies the given timezones by logpoint. Obtain the value of the available timezones using Timezone - List API. Optional Field

Request Example

```
{
   "data": {
      "availability": "Minimal",
      "confidentiality": "Minimal",
      "devicegroup": [
         "574fb123d8aaa4625bfe2d23"
      ],
      "distributed_collector": [
         "5db02cbcd8aaa42fddb6f72f"
      ],
      "integrity": "Minimal",
      "ip": [
         "192.168.1.2",
         "google.com"
      ],
      "logpolicy": [
         "5d88c559d8aaa42d8c4bfc41"
      ],
      "name": "device1",
      "timezone": "Asia/Kathmandu"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

9.6 Devices - Get

Fetches the device with given ID.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Devices/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	ID of the existing device that you want to fetch.

Success Response

```
{
   "active": true,
   "col_apps": [],
   "device_groups": [
      "62e8a1f2785762f6c5f2d372"
   ],
   "distributed_collector": [],
   "has_hostname": true,
   "id": "63da2ac979385684d98f4263",
   "ip": [
      "192.168.2.10",
      "google.com"
   ],
   "log_policies": [],
   "name": "device1",
   "risk_values": {
      "availability": "Minimal",
      "confidentiality": "Minimal",
      "integrity": "Minimal"
   },
   "tid": "",
   "timezone": "Asia/Kathmandu",
   "type": null
}
```

9.7 Devices - GetPlugins

Fetches plugins with given Device ID.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Devices/{id}/plugins
```

Parameter

Field	Label in UI	Type	Description
id	-	String	ID of the existing device whose plugin you want to fetch.

Success Response

```
[
    {
        "CSRFToken": "cknHNJFOKZGrCfm",
        "LOGGEDINUSER": "admin",
        "app": "SnareCollector",
        "charset": "utf_8",
        "hasLCP": "0",
        "ips": "181.170.0.101",
        "normalizer": "None",
        "parser": "LineParser",
        "repo": "default",
        "requestType": "formsubmit",
        "sid": "snare|device-NewDevice_101"
    },
    {
        "CSRFToken": "cknHNJFOKZGrCfm",
        "LOGGEDINUSER": "admin",
        "app": "SyslogCollector",
        "charset": "utf_8",
        "hasLCP": "0",
        "ips": "181.170.0.101",
        "normalizer": "None",
        "parser": "SyslogParser",
        "proxy_condition": "None",
        "repo": "default",
        "requestType": "formsubmit",
        "sid": "syslog|device-NewDevice_101"
    }
]
```

9.8 Devices - Install

Install a given CSV file containing devices

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Devices/install
```

Parameter

Field	Label in UI	Type	Description
file_location	-	String	Location of the file uploaded to install. Can be either 'private' or 'public'. Mandatory Field
file_name	-	String	Name of the CSV file containing Devices. Mandatory Field

Request Example

```
{
   "data": {
      "file_location": "private",
      "file_name": "devices.csv"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

9.9 Devices - List

Lists all devices in the Fabric-enabled LogPoint.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Devices
```

Success Response

```
[
   {
      "active": true,
      "col_apps": [
         {
            "app": "SCPFetcher",
            "auth_password": "CvG244MgnWCj2qcacCeBnO1JUfXCICFvU3gs7eXXfzw=",
            "auth_type": "password",
            "charset": "ascii",
            "interval": "9",
            "namepattern": "*.pyc",
            "parser": "SyslogParser",
```

(continues on next page)

(continued from previous page)

```
                "port": "22",
                "processpolicy": "62e8a1f2785762f6c5f2d36c",
                "remotepath": "C:\\\\test\\\\folder",
                "sid": "scp|device-device4:SCPTest:22:C:\\\\test\\\\folder:*.pyc",
                "username": "SCPTest",
                "uuid": "25efde05c2174722a1f6dc7642b4f4b2"
            },
            {
                "app": "FTPFetcher",
                "charset": "ascii",
                "interval": "34",
                "namepattern": "*.pyc",
                "oldlogs": "off",
                "parser": "SyslogParser",
                "password": "YaNEZM5wl6ffOp73bEc/wrPQxv94QsvWP8lncT3C+is=",
                "port": "33",
                "processpolicy": "62e8a1f2785762f6c5f2d36c",
                "remotepath": "/base/collection/",
                "sid": "ftpf|device-device4:ftptest:33:/base/collection/:*.pyc",
                "username": "FTPtest",
                "uuid": "39154458f8494d0dbd70f5df40d9215d"
            }
        ],
        "device_groups": [
            "62e8a1f2785762f6c5f2d372"
        ],
        "distributed_collector": [],
        "has_hostname": true,
        "id": "63da2ae41547b9cbd69b3f7f",
        "ip": [
            "192.168.2.11",
            "google.com"
        ],
        "log_policies": [],
        "name": "device4",
        "risk_values": {
            "availability": "Minimal",
            "confidentiality": "Minimal",
            "integrity": "Minimal"
        },
        "tid": "",
        "timezone": "Asia/Kathmandu",
        "type": null
    }
]
```

9.10 Devices - ListBlockedIps

Lists the IPs of all the devices in the blocked IP list.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Devices/blockedips
```

Success Response

```
[
    {
        "collected_at": "LogPoint204",
        "ip": "10.45.3.218",
        "name": "10_45_3_218"
    }
]
```

9.11 Devices - ListIgnoredIps

Lists the IPs of all the devices in the ignored IP list.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Devices/ignoredips
```

Success Response

```
[
    {
        "id": "5a1fd832d8aaa41eeee5e5cf",
        "ips": [
            "10.94.0.142"
        ]
    },
    {
        "id": "5a2521fdd8aaa41eeee5e5d2",
        "ips": [
            "10.94.1.22"
        ]
    },
    {
        "id": "5a2521ffd8aaa41eeee5e5d3",
        "ips": [
            "10.94.0.82"
```

(continues on next page)

(continued from previous page)

```
        ]
    }
]
```

9.12 Devices - ListPrivateUploads

List all the csv files that contains device configurations in private storage

GET

```
https://api-server-host-name/configapi/{pool_UUID}/Devices/list
```

Success Response

```
[
    "devices.csv"
]
```

9.13 Devices - ListPublicUploads

List all the csv files that contains device configurations in public storage

GET

```
https://api-server-host-name/configapi/Devices/list
```

Success Response

```
[
    "devices.csv"
]
```

9.14 Devices - RefreshBlockedIpsList

Updates the blocked IP list.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Devices/
↪detectblockedips/refreshlist
```

Request Example

```
{
    "data": {}
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

9.15 Devices - Trash

Removes the device with given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Devices/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	ID of the existing device that you want to delete. Mandatory Field

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

9.16 Devices - TrashIgnoredIps

Removes any device IP with given ID from the ignored IP list.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Devices/{id}/
↪ignoredips
```

Parameter

Field	Label in UI	Type	Description
id	-	String	ID of the ignored IP address that you want to remove from the Ignored IP List. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

9.17 Devices - TrashPrivateUploads

Delete the file with given name from private storage

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/Devices/{file_name}
```

Parameter

Field	Label in UI	Type	Description
file_name		String	Name of the file to be deleted. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "devices.csv successfully deleted"
}
```

9.18 Devices - TrashPublicUploads

Delete the file with given name from public storage

DELETE

```
https://api-server-host-name/configapi/Devices/{file_name}
```

Parameter

Field	Label in UI	Type	Description
file_name		String	Name of the file to be deleted. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "devices.csv successfully deleted"
}
```

9.19 Devices - Upload

Upload csv file containing device configurations to private storage.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/Devices/upload
```

Header

Field	Label in UI	Description
file_name		Name of the file to be uploaded.
Content-Type		application/octet-stream
replace_existing		Set the value of this parameter as 'true' to replace the existing file with the same name with the new file. Default value is 'false'. Value can be 'true' or 'false'. Optional field

Parameter

Field	Label in UI	Type	Description
file		[Object]	(csv) to be uploaded. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "devices.csv successfully uploaded in private storage. "
}
```

9.20 Devices - UploadPublic

Upload csv file containing device configurations to private storage.

POST

```
https://api-server-host-name/configapi/Devices/publicupload
```

Header

Field	Label in UI	Description
file_name		Name of the file to be uploaded.
Content-Type		application/octet-stream
replace_existing		Set the value of this parameter as 'true' to replace the existing file with the same name with the new file. Default value is 'false'. Value can be 'true' or 'false'. Optional field

Parameter

Field	Label in UI	Type	Description
file		[Object]	(csv) to be uploaded. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "devices.csv successfully uploaded in public storage."
}
```

CHAPTER

TEN

DIAGNOSIS

10.1 Diagnosis - GetDirectorDiagnosisAPIStat

Fetches the system diagnostic information of API server.

GET

```
https://api-server-host-name/monitorapi/v1/director/diagnosis/api/stat?metrics={metrics_name}
```

Parameter

Field	Label in UI	Type	Description
metrics		String	Query string specifying to retrieve data for specific metrics. Optional Field.

Success Response

```
[
  {
    "api16.logpoint.local": {
      "1594180200": {
        "zpoolStatistics": [
          {
            "name": "app_pool",
            "health": "ONLINE",
            "diskAllocation": "3.56G",
            "freeDisk": "26.2G",
            "readOperations": "28",
            "writeOperations": "7",
            "readBandwidth": "516K",
            "writeBandwidth": "148K",
            "failedDisks": []
          },
```

(continues on next page)

(continued from previous page)

```
      {
        "name": "data_pool",
        "health": "ONLINE",
        "diskAllocation": "22.2M",
        "freeDisk": "25.7G",
        "readOperations": "2",
        "writeOperations": "4",
        "readBandwidth": "30.0K",
        "writeBandwidth": "69.2K",
        "failedDisks": []
      },
      {
        "name": "rpool",
        "health": "ONLINE",
        "diskAllocation": "3.32G",
        "freeDisk": "20.6G",
        "readOperations": "12",
        "writeOperations": "9",
        "readBandwidth": "419K",
        "writeBandwidth": "157K",
        "failedDisks": []
      }
    ],
    "hardware": "VMware, Inc., VMware Virtual Platform",
    "serialNumber": "VMware-42 33 c8 63 ab ef e3 db-85 ba 1e b2 2c 19 dd 29",
    "diskUsage": [
      {
        "filesystem": "rpool/ROOT/com_root",
        "size": "19G",
        "used": "3.4G",
        "available": "16G",
        "usedPercentage": "18",
        "mountedOn": "/"
      },
      {
        "filesystem": "app_pool/application",
        "size": "29G",
        "used": "3.6G",
        "available": "26G",
        "usedPercentage": "13",
        "mountedOn": "/opt/commander"
      },
      {
        "filesystem": "data_pool/bigstore",
        "size": "25G",
```

(continues on next page)

(continued from previous page)

```
                        "used": "21M",
                        "available": "25G",
                        "usedPercentage": "1",
                        "mountedOn": "/opt/commander/bigstore"
                    },
                    {
                        "filesystem": "total",
                        "size": "73G",
                        "used": "6.9G",
                        "available": "66G",
                        "usedPercentage": "10",
                        "mountedOn": "-"
                    }
                ],
                "numberOfCores": "4",
                "memoryUsageInMb": {
                    "totalMemory": 7983,
                    "inactiveMemory": 110,
                    "freeMemory": 5375,
                    "availableMemory": 5361
                },
                "idlePercentage": "88.70",
                "ioWait": {
                    "value": 3.53,
                    "message": "High disk IO load: 3.53... It may be necessary to distribute the disk IO to more drives or limit the amount of logs"
                },
                "loadAverage": {
                    "value": 0.48,
                    "message": "No CPU load problems detected"
                },
                "kernelSwap": {
                    "value": "60",
                    "message": "Kernel Swap Info:vm.swappiness = 60 - please set it to 1 by adding vm.swappiness=1 to /etc/sysctl.conf and set it using sysctl vm.swappiness=1"
                },
                "swappingIoInMb": {
                    "value": 0.0,
                    "message": "No memory problems detected"
                },
                "diagnosticsVersion": "2.0.0"
            }
        }
    }
]
```

10.2 Diagnosis - GetDirectorDiagnosisFabricStat

Fetches the system diagnostic information of Fabric server(s).

GET

```
https://api-server-host-name/monitorapi/v1/director/diagnosis/fabric/stat?metrics={metrics_
↪name}
```

Parameter

Field	Label in UI	Type	Description
metrics		String	Query string specifying to retrieve data for specific metrics. Optional Field.

Success Response

```
[
    {
        "fabric15.logpoint.local": {
            "1596546000": {
                "fabricServerCount": 1,
                "fabricProxyService": "active",
                "fabricProxyServerState": "standalone",
                "fabricProxyNumAliveConnections": "18",
                "fabricProxyZnodeCount": "667",
                "fabricProxyAvgLatency": "0",
                "fabricProxyMaxLatency": "288",
                "fabricProxyMinLatency": "0",
                "fabricProxyOpenFileDescriptorCount": "54",
                "fabricProxyMaxFileDescriptorCount": "4096",
                "fabricStorageTotalCapacity": null,
                "fabricStoragePresentCapacity": null,
                "fabricStorageUsedPercent": null,
                "underReplicatedBlocks": null,
                "liveDatanodes": null,
                "fabAuthService": "active",
                "fabAuthAdminService": "active",
                "zpoolStatistics": [
                    {
                        "name": "app_pool",
                        "health": "ONLINE",
                        "diskAllocation": "325M",
                        "freeDisk": "29.4G",
                        "readOperations": "0",
```

(continues on next page)

(continued from previous page)

```
            "writeOperations": "1",
            "readBandwidth": "2.22K",
            "writeBandwidth": "17.6K",
            "failedDisks": []
          },
          {
            "name": "data_pool",
            "health": "ONLINE",
            "diskAllocation": "167M",
            "freeDisk": "25.6G",
            "readOperations": "0",
            "writeOperations": "1",
            "readBandwidth": "822",
            "writeBandwidth": "23.7K",
            "failedDisks": []
          },
          {
            "name": "rpool",
            "health": "ONLINE",
            "diskAllocation": "3.32G",
            "freeDisk": "20.6G",
            "readOperations": "0",
            "writeOperations": "8",
            "readBandwidth": "2.91K",
            "writeBandwidth": "158K",
            "failedDisks": []
          }
        ],
        "hardware": "VMware, Inc., VMware Virtual Platform",
        "serialNumber": "VMware-42 33 d5 67 f4 72 d5 51-68 7d a3 6c 32 b5 3f 8b",
        "diskUsage": [
          {
            "filesystem": "rpool/ROOT/com_root",
            "size": "19G",
            "used": "3.4G",
            "available": "16G",
            "usedPercentage": "18",
            "mountedOn": "/"
          },
          {
            "filesystem": "app_pool/application",
            "size": "29G",
            "used": "324M",
            "available": "29G",
            "usedPercentage": "2",
```

(continues on next page)

(continued from previous page)

```
            "mountedOn": "/opt/commander"
          },
          {
            "filesystem": "data_pool/bigstore",
            "size": "25G",
            "used": "165M",
            "available": "25G",
            "usedPercentage": "1",
            "mountedOn": "/opt/commander/bigstore"
          },
          {
            "filesystem": "total",
            "size": "73G",
            "used": "3.8G",
            "available": "69G",
            "usedPercentage": "6",
            "mountedOn": "-"
          }
        ],
        "numberOfCores": "4",
        "memoryUsageInMb": {
          "totalMemory": 7983,
          "inactiveMemory": 74,
          "freeMemory": 5693,
          "availableMemory": 5601
        },
        "idlePercentage": "95.80",
        "ioWait": {
          "value": 2.45,
          "message": "High disk IO load: 2.45... It may be necessary to distribute the disk IO
↪to more drives or limit the amount of logs"
        },
        "loadAverage": {
          "value": 0.13,
          "message": "No CPU load problems detected"
        },
        "kernelSwap": {
          "value": "60",
          "message": "Kernel Swap Info:vm.swappiness = 60 - please set it to 1 by adding vm.
↪swappiness=1 to /etc/sysctl.conf and set it using sysctl vm.swappiness=1"
        },
        "swappingIoInMb": {
          "value": 0.0,
          "message": "No memory problems detected"
        },
```

(continues on next page)

(continued from previous page)

```
        "diagnosticsVersion": "2.0.0"
      }
    }
  }
]
```

10.3 Diagnosis - GetDirectorDiagnosisLPSMStat

Fetches the system diagnostic information of LPSM server.

GET

```
https://api-server-host-name/monitorapi/v1/director/diagnosis/lpsm/stat?metrics={metrics_
↪name}
```

Parameter

Field	Label in UI	Type	Description
metrics		String	Query string specifying to retrieve data for specific metrics. Optional Field.

Success Response

```
[
  {
    "lpsm236.logpoint.com": {
      "1594181700": {
        "lpsmVersion": "1.5.0",
        "hardware": "VMware, Inc., VMware Virtual Platform",
        "serialNumber": "VMware-42 33 02 b9 2a 4d 52 97-6d b8 ad 17 b4 be 20 78",
        "diskUsage": [
          {
            "filesystem": "rpool/ROOT/lp_root",
            "size": "19G",
            "used": "3.3G",
            "available": "16G",
            "usedPercentage": "18",
            "mountedOn": "/"
          },
          {
            "filesystem": "app_pool/application",
            "size": "9.7G",
```

(continues on next page)

(continued from previous page)

```
                "used": "2.5G",
                "available": "7.2G",
                "usedPercentage": "26",
                "mountedOn": "/opt"
            },
            {
                "filesystem": "app_store_pool/app_store",
                "size": "9.7G",
                "used": "20M",
                "available": "9.7G",
                "usedPercentage": "1",
                "mountedOn": "/opt/makalu/app_store"
            },
            {
                "filesystem": "data_pool/storage",
                "size": "35G",
                "used": "896K",
                "available": "35G",
                "usedPercentage": "1",
                "mountedOn": "/opt/makalu/storage"
            },
            {
                "filesystem": "total",
                "size": "73G",
                "used": "5.8G",
                "available": "68G",
                "usedPercentage": "8",
                "mountedOn": "-"
            }
        ],
        "zpoolStatistics": [
            {
                "name": "app_pool",
                "diskAllocation": "2.46G",
                "freeDisk": "7.48G",
                "readOperations": "0",
                "writeOperations": "4",
                "readBandwidth": "7.22K",
                "writeBandwidth": "77.2K",
                "health": "ONLINE",
                "failedDisks": []
            },
            {
                "name": "app_store_pool",
                "diskAllocation": "20.2M",
```

(continues on next page)

(continued from previous page)

```
            "freeDisk": "9.92G",
            "readOperations": "0",
            "writeOperations": "0",
            "readBandwidth": "234",
            "writeBandwidth": "221",
            "health": "ONLINE",
            "failedDisks": []
          },
          {
            "name": "data_pool",
            "diskAllocation": "1.89M",
            "freeDisk": "35.7G",
            "readOperations": "0",
            "writeOperations": "0",
            "readBandwidth": "242",
            "writeBandwidth": "8.29K",
            "health": "ONLINE",
            "failedDisks": []
          },
          {
            "name": "rpool",
            "diskAllocation": "3.24G",
            "freeDisk": "20.6G",
            "readOperations": "1",
            "writeOperations": "7",
            "readBandwidth": "30.8K",
            "writeBandwidth": "157K",
            "health": "ONLINE",
            "failedDisks": []
          }
        ],
        "numberOfCores": "4",
        "memoryUsageInMb": {
          "totalMemory": 7983,
          "inactiveMemory": 81,
          "freeMemory": 5982,
          "availableMemory": 5925
        },
        "idlePercentage": "98.64",
        "ioWait": {
          "value": "2.1",
          "message": "High disk IO load: 2.1... It may be necessary to distribute the disk IO
↪to more drives or limit the amount of logs"
        },
        "loadAverage": {
```

(continues on next page)

(continued from previous page)

```
                "value": "0.01",
                "message": "No CPU load problems detected"
            },
            "swappingIoInMb": {
                "value": 0.0,
                "message": "No memory problems detected"
            },
            "kernelSwap": {
                "value": "60",
                "message": "Kernel Swap Info:vm.swappiness = 60 - please set it to 1 by adding vm.swappiness=1 to /etc/sysctl.conf and set it using sysctl vm.swappiness=1"
            },
            "messageQueueStatistics": {
                "nodeName": "lpsm-messaging-server@localhost",
                "totalConsumers": 5,
                "totalQueues": 5,
                "totalExchanges": 21,
                "totalConnections": 2,
                "totalChannels": 4,
                "queueTotalMessages": 0,
                "queueTotalMessagesReady": 0,
                "queueTotalMessagesUnacknowledged": 0,
                "messagesPublished": 3844,
                "messagesDelivered": 3845,
                "running": true,
                "uptime": 7747027,
                "osPid": "7906",
                "diskFree": 16792682496,
                "diskFreeLimit": 50000000,
                "diskFreeAlarm": false,
                "vmMemoryLimit": 3348401356,
                "memUsed": 53996576,
                "memAlarm": false,
                "processLimit": 1048576,
                "fdTotal": 65536,
                "fdUsed": 26,
                "socketsTotal": 58890,
                "socketsUsed": 3,
                "procUsed": 217,
                "queuesNotRunning": ""
            },
            "services": [
                {
                    "name": "incoherent_updater",
                    "cpu": 0.0,
```

(continues on next page)

(continued from previous page)

```
                    "memory": 0.27,
                    "status": "up"
                },
                {
                    "name": "support_con_client",
                    "cpu": 0.0,
                    "memory": 0.06,
                    "status": "up"
                },
                {
                    "name": "commander_vpnclient",
                    "cpu": 0.0,
                    "memory": 0.06,
                    "status": "up"
                },
                {
                    "name": "jobprocessor",
                    "cpu": 0.0,
                    "memory": 0.24,
                    "status": "up"
                },
                {
                    "name": "msui_cleaner",
                    "cpu": 0.0,
                    "memory": 0.27,
                    "status": "up"
                },
                {
                    "name": "system_notifications",
                    "cpu": 0.0,
                    "memory": 0.32,
                    "status": "up"
                },
                {
                    "name": "mongodb",
                    "cpu": 0.0,
                    "memory": 0.74,
                    "status": "up"
                },
                {
                    "name": "webserver",
                    "cpu": 0.0,
                    "memory": 0.28,
                    "status": "up"
                },
```

(continues on next page)

(continued from previous page)

```
                    {
                        "name": "pool_reader",
                        "cpu": 0.0,
                        "memory": 0.35,
                        "status": "up"
                    },
                    {
                        "name": "support_connection_timeout",
                        "cpu": 0.0,
                        "memory": 0.25,
                        "status": "up"
                    },
                    {
                        "name": "system_metrics",
                        "cpu": 0.0,
                        "memory": 0.28,
                        "status": "up"
                    }
                ],
                "diagnosticsVersion": "2.0.0"
            }
        }
    }
]
```

10.4 Diagnosis - GetDirectorHealth

Fetches the health status on the basis of version compatibility of the API Server and the Fabric Server(s).

GET

```
https://api-server-host-name/monitorapi/v1/director/health
```

Success Response

```
{
    "version": {
        "message": "All the Fabric and API servers are in same version.",
        "status": "OK"
    }
}
```

10.5 Diagnosis - GetDirectorVersion

Fetches the current version of the Director Components.

GET

```
https://api-server-host-name/monitorapi/v1/director/version
```

Success Response

```
{
   "fabric": {
      "fabric12.logpoint.local": "1.2.0",
      "fabric10.logpoint.local": "1.2.0",
      "fabric11.logpoint.local": "1.2.0"
   },
   "api": {
      "api13.logpoint.local": "1.2.0"
   },
   "lpsm": {
      "lpsm9-14": "1.0.1"
   }
}
```

10.6 Diagnosis - GetLogpointDiagnosisJava

Fetches the java_memory diagnostic information of Logpoint.

GET

```
https://api-server-host-name/monitorapi/v1/{pool_UUID}/{logpoint_identifier}/diagnosis/java?
↪metrics={metrics}
```

Parameter

Field	Label in UI	Type	Description
metrics		String	Query string specifying to retrieve data for specific metrics. Optional Field.

Success Response

```
[
   {
      "b5ac4e99fc724ec7ba2081f4eed87c19": {
```

(continues on next page)

(continued from previous page)

```
      "c7e0c00da17c407499a76f21a09a9720": {
        "1594278000": {
          "javaProcesses": [
            {
              "processName": "file_keeper__logpoint",
              "pid": "15425",
              "message": []
            },
            {
              "processName": "indexsearcher_default",
              "pid": "15494",
              "message": [
                "Young GC is too slow, takes: 0.13816666666666666 millisecs (avg), sb. no
↪more than 50 ms in avg"
              ]
            },
            {
              "processName": "premerger",
              "pid": "15431",
              "message": [
                "Young GC is too slow, takes: 0.26836363636363636 millisecs (avg), sb. no
↪more than 50 ms in avg"
              ]
            },
            {
              "processName": "lookup_populator",
              "pid": "15496",
              "message": []
            },
            {
              "processName": "enrichment_service",
              "pid": "15435",
              "message": []
            },
            {
              "processName": "file_keeper__LogPointAlerts",
              "pid": "15501",
              "message": [
                "Young GC is too slow, takes: 0.218 millisecs (avg), sb. no more than 50 ms in
↪avg"
              ]
            },
            {
              "processName": "analyzer",
              "pid": "15410",
```

(continues on next page)

(continued from previous page)

```
                "message": []
            },
            {
                "processName": "lookup_indexsearcher",
                "pid": "15350",
                "message": []
            },
            {
                "processName": "merger",
                "pid": "15513",
                "message": [
                    "Young GC is too slow, takes: 0.1545 millisecs (avg), sb. no more than 50 ms
↪in avg"
                ]
            },
            {
                "processName": "indexsearcher__LogPointAlerts",
                "pid": "15322",
                "message": [
                    "Young GC is too slow, takes: 0.14079999999999998 millisecs (avg), sb. no
↪more than 50 ms in avg"
                ]
            },
            {
                "processName": "file_keeper_default",
                "pid": "15514",
                "message": [
                    "Young GC is too slow, takes: 0.46533333333333333 millisecs (avg), sb. no
↪more than 50 ms in avg"
                ]
            },
            {
                "processName": "dynamic_entity_service",
                "pid": "15515",
                "message": [
                    "Young GC is too slow, takes: 0.662 millisecs (avg), sb. no more than 50 ms in
↪avg"
                ]
            },
            {
                "processName": "labeling",
                "pid": "15421",
                "message": []
            },
            {
```

(continues on next page)

(continued from previous page)

```
                            "processName": "indexsearcher__logpoint",
                            "pid": "15423",
                            "message": []
                        }
                    ],
                    "diagnosticsVersion": "2.0.0"
                }
            }
        }
    }
]
```

10.7 Diagnosis - GetLogpointDiagnosisNormFront

Fetches the normm front diagnostic information of Logpoint.

GET

```
https://api-server-host-name/monitorapi/v1/{pool_UUID}/{logpoint_identifier}/diagnosis/norm_
↪front?metrics={metrics}
```

Parameter

Field	Label in UI	Type	Description
metrics		String	Query string specifying to retrieve data for specific metrics. Optional Field.

Success Response

```
[
    {
        "b5ac4e99fc724ec7ba2081f4eed87c19": {
            "c7e0c00da17c407499a76f21a09a9720": {
                "1594278000": {
                    "actualEps": 0,
                    "averageEps": 0,
                    "totalQueueSizeInBytes": 0.0,
                    "affectedProcesses": [],
                    "diagnosticsVersion": "2.0.0"
                }
            }
        }
```

(continues on next page)

(continued from previous page)

```
  }
]
```

10.8 Diagnosis - GetLogpointDiagnosisNormalisers

Fetches the normalisers diagnostic information of Logpoint.

GET

```
https://api-server-host-name/monitorapi/v1/{pool_UUID}/{logpoint_identifier}/diagnosis/
↪normalisers?metrics={metrics}
```

Parameter

Field	Label in UI	Type	Description
metrics		String	Query string specifying to retrieve data for specific metrics. Optional Field.

Success Response

```
[
  {
    "b5ac4e99fc724ec7ba2081f4eed87c19": {
      "c7e0c00da17c407499a76f21a09a9720": {
        "1594278000": {
          "configuredNormalizers": null,
          "activeNormalizers": 4,
          "averageNormalizerLoadinCpuPercentage": 0.1,
          "totalDoableEps": 0,
          "averageDoableEps": 0,
          "totalActualEps": 0,
          "averageActualEps": 0,
          "message": [],
          "totalQueueSizeInBytes": 0.0,
          "affectedProcesses": [],
          "diagnosticsVersion": "2.0.0"
        }
      }
    }
  }
]
```

10.9 Diagnosis - GetLogpointDiagnosisPremerger

Fetches the premerger diagnostic information of Logpoint.

GET

```
https://api-server-host-name/monitorapi/v1/{pool_UUID}/{logpoint_identifier}/diagnosis/
↪premerger?metrics={metrics}
```

Parameter

Field	Label in UI	Type	Description
metrics		String	Query string specifying to retrieve data for specific metrics. Optional Field.

Success Response

```
[
    {
        "b5ac4e99fc724ec7ba2081f4eed87c19": {
            "c7e0c00da17c407499a76f21a09a9720": {
                "1594278000": {
                    "completeWidgets": 1,
                    "incompleteWidgets": 0,
                    "message": [
                        "Widget completion looks fine!!"
                    ],
                    "incompleteLiveSearches": [],
                    "diagnosticsVersion": "2.0.0"
                }
            }
        }
    }
]
```

10.10 Diagnosis - GetLogpointDiagnosisStat

Fetches the system diagnostic information of Logpoint.

GET

```
https://api-server-host-name/monitorapi/v1/{pool_UUID}/{logpoint_identifier}/diagnosis/stat?
↪metrics={metrics}
```

Parameter

Field	Label in UI	Type	Description
metrics		String	Query string specifying to retrieve data for specific metrics. Optional Field.

Success Response

```
[
  {
    "b5ac4e99fc724ec7ba2081f4eed87c19": {
      "c7e0c00da17c407499a76f21a09a9720": {
        "1594202400": {
          "logPointVersion": "7.1.0.339",
          "openFiles": 13546,
          "hardware": "VMware, Inc., VMware Virtual Platform",
          "serialNumber": "VMware-42 33 31 1b 81 eb 1c 8a-6e db c2 30 50 44 ec 17",
          "diskUsage": [
            {
              "filesystem": "rpool/ROOT/lp_root",
              "size": "19G",
              "used": "4.3G",
              "available": "15G",
              "usedPercentage": "23",
              "mountedOn": "/"
            },
            {
              "filesystem": "app_pool/application",
              "size": "9.7G",
              "used": "2.0G",
              "available": "7.7G",
              "usedPercentage": "21",
              "mountedOn": "/opt"
            },
            {
              "filesystem": "app_store_pool/app_store",
              "size": "9.7G",
              "used": "113M",
              "available": "9.6G",
              "usedPercentage": "2",
              "mountedOn": "/opt/makalu/app_store"
            },
            {
              "filesystem": "data_pool/storage",
              "size": "35G",
              "used": "410M",
              "available": "35G",
```

(continues on next page)

(continued from previous page)

```
                        "usedPercentage": "2",
                        "mountedOn": "/opt/makalu/storage"
                    },
                    {
                        "filesystem": "total",
                        "size": "73G",
                        "used": "6.8G",
                        "available": "67G",
                        "usedPercentage": "10",
                        "mountedOn": "-"
                    }
                ],
                "zpoolStatistics": [
                    {
                        "name": "app_pool",
                        "diskAllocation": "2.00G",
                        "freeDisk": "7.94G",
                        "readOperations": "0",
                        "writeOperations": "9",
                        "readBandwidth": "4.81K",
                        "writeBandwidth": "177K",
                        "health": "ONLINE",
                        "failedDisks": []
                    },
                    {
                        "name": "app_store_pool",
                        "diskAllocation": "121M",
                        "freeDisk": "9.82G",
                        "readOperations": "0",
                        "writeOperations": "3",
                        "readBandwidth": "1.86K",
                        "writeBandwidth": "69.0K",
                        "health": "ONLINE",
                        "failedDisks": []
                    },
                    {
                        "name": "data_pool",
                        "diskAllocation": "419M",
                        "freeDisk": "35.3G",
                        "readOperations": "0",
                        "writeOperations": "6",
                        "readBandwidth": "898",
                        "writeBandwidth": "158K",
                        "health": "ONLINE",
                        "failedDisks": []
```

(continues on next page)

(continued from previous page)

```
                },
                {
                    "name": "rpool",
                    "diskAllocation": "4.25G",
                    "freeDisk": "19.6G",
                    "readOperations": "0",
                    "writeOperations": "9",
                    "readBandwidth": "11.7K",
                    "writeBandwidth": "179K",
                    "health": "ONLINE",
                    "failedDisks": []
                }
            ],
            "numberOfCores": "4",
            "memoryUsageInMb": {
                "totalMemory": 7976,
                "inactiveMemory": 240,
                "freeMemory": 563,
                "availableMemory": 669
            },
            "idlePercentage": "89.20",
            "ioWait": {
                "value": "1.34",
                "message": "High disk IO load: 1.34... It may be necessary to distribute the disk
↪IO to more drives or limit the amount of logs"
            },
            "loadAverage": {
                "value": "0.59",
                "message": "No CPU load problems detected"
            },
            "swappingIoInMb": {
                "value": 0.0,
                "message": "No memory problems detected"
            },
            "kernelSwap": {
                "value": "60",
                "message": "Kernel Swap Info:vm.swappiness = 60 - please set it to 1 by adding
↪vm.swappiness=1 to /etc/sysctl.conf and set it using sysctl vm.swappiness=1"
            },
            "serviceLayers": {
                "collection": {
                    "cpu": 0.0,
                    "memory": 1519.52,
                    "queue": 0
                },
```

(continues on next page)

(continued from previous page)

```
        "normalization": {
            "cpu": 2.0,
            "memory": 4.55,
            "queue": 0
        },
        "enrichment": {
            "cpu": 0.0,
            "memory": 9.66,
            "queue": 0
        },
        "indexing": {
            "cpu": 1.0,
            "memory": 19.360000000000003,
            "queue": 0
        },
        "liveSearch": {
            "cpu": 0.0,
            "memory": 7.07,
            "storage": 2.47
        }
    },
    "stoppedServices": [
        "remote_con_server"
    ],
    "repoDiskUsage": [
        {
            "repoName": "default",
            "currentUsageInMb": "0.74805",
            "logSizeYesterdayInMb": 0,
            "logSizeLastMonthInMb": 0
        },
        {
            "repoName": "_logpoint",
            "currentUsageInMb": "383.72363",
            "logSizeYesterdayInMb": 0,
            "logSizeLastMonthInMb": 0
        },
        {
            "repoName": "_LogPointAlerts",
            "currentUsageInMb": "0.05176",
            "logSizeYesterdayInMb": null,
            "logSizeLastMonthInMb": null
        }
    ],
    "diagnosticsVersion": "2.0.0"
```

(continues on next page)

(continued from previous page)

```
                }
            }
        }
    }
]
```

10.11 Diagnosis - GetLogpointDiagnosisStoreHandler

Fetches the store handler diagnostic information of Logpoint.

GET

```
https://api-server-host-name/monitorapi/v1/{pool_UUID}/{logpoint_identifier}/diagnosis/store_
↪handler?metrics={metrics}
```

Parameter

Field	Label in UI	Type	Description
metrics		String	Query string specifying to retrieve data for specific metrics. Optional Field.

Success Response

```
[
    {
        "b5ac4e99fc724ec7ba2081f4eed87c19": {
            "c7e0c00da17c407499a76f21a09a9720": {
                "1594278000": {
                    "actualEps": 0,
                    "averageEps": 0,
                    "totalQueueSizeInBytes": 0.0,
                    "affectedProcesses": [],
                    "diagnosticsVersion": "1.0.0"
                }
            }
        }
    }
]
```

10.12 Diagnosis - GetPoolInfo

Fetches pool and machine information.

GET

```
https://api-server-host-name/monitorapi/v1/director/poolinfo
```

Success Response

```
[
    {
        "active": true,
        "machines": [
            {
                "director_mode": "fabric_only",
                "identifier": "2ea122a7bea4451b855967837d552a78",
                "name": "LogPoint",
                "version": "6.11.0"
            }
        ],
        "name": "Pool1",
        "pool_uuid": "99e45a6941d0435dab3133f603e41303"
    },
    {
        "active": false,
        "machines": [],
        "name": "Pool2",
        "pool_uuid": "513345eef98440df903457a5370d1233"
    }
]
```

CHAPTER

ELEVEN

DISTRIBUTEDCOLLECTORS

11.1 DistributedCollectors - Activate

Activates a distributed collector.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/DistributedCollectors/
↪{id}/activate
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing distributed collector ID. Execute DistributedCollectors - List API to obtain the id of required Distributed Collector. Mandatory Field

Request Example

```
{
   "data": {}
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

11.2 DistributedCollectors - Deactivate

Deactivate a distributed collector.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/DistributedCollectors/
↪{id}/deactivate
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing distributed collector ID. Execute DistributedCollectors - List API to obtain the id of required Distributed Collector. Mandatory Field

Request Example

```
{
    "data": {}
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

11.3 DistributedCollectors - Get

Fetches a distributed collector with given ID.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/DistributedCollectors/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing distributed collector ID. Execute DistributedCollectors - List API to obtain the id of required Distributed Collector.

Success Response

```
{
    "active": true,
    "buffering": true,
    "description": "",
    "file_socket_port": 6900,
    "id": "59b62b15d8aaa4245809137f",
    "identifier": "a8131f6cfb314e87b7cfdaedfee238a0",
    "ip": "192.168.100.79",
    "is_li_light": true,
    "name": "LogPoint79",
    "tid": ""
}
```

11.4 DistributedCollectors - List

Lists all distributed collectors.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/DistributedCollectors
```

Success Response

```
[
    [
        {
            "active": true,
            "buffering": false,
            "description": "",
            "file_socket_port": 6900,
            "id": "59086b2e854ff52ff3344eb5",
            "identifier": "e2bb6740612049929b89a559043522f3",
            "ip": "10.45.1.188",
            "is_li_light": true,
            "name": "LogPoint",
            "tid": ""
        }
```

(continues on next page)

(continued from previous page)

```
    ]
]
```

11.5 DistributedCollectors - RefreshList

Refresh the list to sync distributed collector data.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/DistributedCollectors/
↪refreshlist
```

Request Example

```
{
    "data": {}
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

11.6 DistributedCollectors - Trash

Deletes a distributed collector with given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/DistributedCollectors/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing distributed collector ID. Execute DistributedCollectors - List API to obtain the id of required Distributed Collector. Mandatory Field

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

TWELVE

DISTRIBUTEDLOGPOINTS

12.1 DistributedLogpoints - Create

Adds a new remote LogPoint.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/DistributedLogpoints
```

Parameter

Field	Label in UI	Type	Description
ip_dns	IP Address or DNS Name	String	IP address of the remote LogPoint. Mandatory Field
password	Password	String	Password for the remote connection provided in the password parameter of the OpenDoor - Create API. Mandatory Field
private_ip	Private IP	String	Private IP address provided in network parameter of the OpenDoor - Create API. Mandatory Field

Request Example

```
{
   "data": {
      "ip_dns": "192.168.2.23",
      "password": "aaaa",
      "private_ip": "10.2.1.1"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

12.2 DistributedLogpoints - Edit

Edits a remote LogPoint with given ID.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/DistributedLogpoints/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	ID of the remote LogPoint. Execute DistributedLogPoints - List API to list the details of all Remote LogPoints. Mandatory Field
ip_dns	IP Address or DNS Name	String	Ip address of the remote LogPoint. Passed as string. Mandatory Field
password	Password	String	Password of the remote LogPoint (during configuring open door at remote LogPoint side). Mandatory Field
private_ip	Private IP	String	Private ip address of the remote LogPoint. Passed as string. Mandatory Field

Request Example

```
{
   "data": {
      "ip_dns": "192.168.2.23",
      "password": "aaaa",
      "private_ip": "10.2.1.1"
   }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

12.3 DistributedLogpoints - Get

Fetches a remote LogPoint with given ID.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/DistributedLogpoints/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing remote LogPoint ID. Use the value of id parameter of the required remote LogPoint from DistributedLogPoints - List API.

Success Response

```
{
    "id": "59100cc2d8aaa439015c8086",
    "is_higher_security_lite": false,
    "name": "",
    "private_ip": "10.2.1.1",
    "remote": "test_DLP_8",
    "status": "Connected",
    "vpn_ip": ""
}
```

12.4 DistributedLogpoints - List

List all remote LogPoints.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/DistributedLogpoints
```

Success Response

```
[
   {
      "id": "59100cc2d8aaa439015c8086",
      "is_higher_security_lite": false,
      "name": "",
      "private_ip": "10.2.1.1",
      "remote": "test_DLP_8",
      "status": "Connected",
      "vpn_ip": ""
   }
]
```

12.5 DistributedLogpoints - RefreshList

Updates the list to sync Distributed Logpoints status data

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/DistributedLogpoints/
↪refreshlist
```

Request Example

```
{
   "data": {}
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

12.6 DistributedLogpoints - Trash

Delete remote LogPoint with given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/DistributedLogpoints/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing remote LogPoint ID. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

THIRTEEN

ENRICHMENTPOLICY

13.1 EnrichmentPolicy - Create

Adds a new enrichment policy.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/EnrichmentPolicy
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing enrichment policy id . Mandatory Field
name	Policy Name	String	Enrichment policy name . Mandatory Field
description	Description	String	Description for the enrichment policy. Optional Field

Continued on next page

Table 1 – continued from previous page

Field	Label in UI	Type	Description
specifications	Specification	[json]	Mandatory Field. The following parameters must be provided to define enrichment policy specifications: **rules**: Rules for the enrichment policy. Optional field. To define rules, the following parameters must be provided: • *category*: Value can be "simple" or "type_based". • *operation*: Value must be "Equals". • *prefix*: Value can be "true" or "false". Mandatory only when category = "type_based". • *event_key*: Event id. Mandatory only when category = "simple". • *source_key*: Source id. • *type*: Value can only be "ip" or "string" or "num". Mandatory only when category = "type_based". **source** : Enrichment

Table 1 – continued from previous page

Field	Label in UI	Type	Description

Request Example

```
{
   "data": {
      "name": "testPolicy",
      "specifications": [
         {
            "rules": [
               {
                  "category": "simple",
                  "source_key": "id",
                  "prefix": false,
                  "operation": "Equals",
                  "type": "string",
                  "event_key": "id"
               }
            ],
            "source": "test_odbc",
            "criteria": [
               {
                  "type": "KeyPresents",
                  "key": "id",
                  "value": ""
               }
            ]
         }
      ],
      "description": "Enrichment Policy <i> description </i>."
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

13.2 EnrichmentPolicy - Edit

Edits an enrichment policy of given id.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/EnrichmentPolicy/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing enrichment policy id . Mandatory Field
name	Policy Name	String	Enrichment policy name . Mandatory Field
description	Description	String	Description for the enrichment policy. Optional Field

Continued on next page

Table 2 – continued from previous page

Field	Label in UI	Type	Description
specifications	Specification	[json]	Mandatory Field. The following parameters must be provided to define enrichment policy specifications: **rules**: Rules for the enrichment policy. Optional field. To define rules, the following parameters must be provided: • *category*: Value can be “simple” or “type_based”. • *operation*: Value must be “Equals”. • *prefix*: Value can be “true” or “false”. Mandatory only when category = “type_based”. • *event_key*: Event id. Mandatory only when category = “simple”. • *source_key*: Source id. • *type*: Value can only be “ip” or “string” or “num”. Mandatory only when category = “type_based”. **source** : Enrichment

Table 2 – continued from previous page

Field	Label in UI	Type	Description

Request Example

```
{
    "data": {
        "name": "testPolicy",
        "description": "Enrichment Policy Description.",
        "specifications": [
            {
                "criteria": [
                    {
                        "type": "KeyPresents",
                        "key": "id",
                        "value": ""
                    }
                ],
                "source": "test_odbc",
                "rules": [
                    {
                        "source_key": "id",
                        "operation": "Equals",
                        "event_key": "id",
                        "category": "simple",
                        "type": "string",
                        "prefix": false
                    }
                ]
            }
        ]
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

13.3 EnrichmentPolicy - Get

Fetches an enrichment policy with given id.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/EnrichmentPolicy/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing Enrichment Policy id .

Success Response

```
{
    "name": "testPolicy",
    "specifications": [
      {
          "rules": [
            {
                "category": "simple",
                "operation": "Equals",
                "prefix": false,
                "event_key": "id",
                "source_key": "id"
            }
          ],
          "source": "test_odbc",
          "criteria": [
            {
                "type": "KeyPresents",
                "key": "id",
                "value": ""
            }
          ]
      }
    ],
    "id": "574fb123d8aaa4625bfe2d23",
    "description": "Enrichment Policy <i> description </i>."
}
```

13.4 EnrichmentPolicy - List

Lists all enrichment policies.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/EnrichmentPolicy
```

Success Response

```
[
    {
        "name": "testPolicy",
        "specifications": [
            {
                "rules": [
                    {
                        "category": "simple",
                        "source_key": "id",
                        "prefix": false,
                        "operation": "Equals",
                        "type": "string",
                        "event_key": "id"
                    }
                ],
                "source": "test_odbc",
                "criteria": [
                    {
                        "type": "KeyPresents",
                        "key": "id",
                        "value": ""
                    }
                ]
            }
        ],
        "id": "574fb123d8aaa4625bfe2d23",
        "description": "Enrichment Policy <i> description </i>."
    }
]
```

13.5 EnrichmentPolicy - Trash

Deletes an enrichment policy with given id.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/EnrichmentPolicy/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Enrichment Policy id . Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

FOURTEEN

ENRICHMENTSOURCE

14.1 EnrichmentSource - Get

Fetches the enrichment source with given ID.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/EnrichmentSource/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing enrichment source id.

Success Response

```
{
  "active": true,
  "delete_status": "",
  "id": "59467646d8aaa41be49d158b",
  "last_updated": 0,
  "plugin_info": {
    "source_fields": [
      {
        "field": "domain"
      },
      {
        "field": "url"
      },
      {
        "field": "category"
      },
      {
        "field": "type"
      },
```

(continues on next page)

(continued from previous page)

```
            {
                "field": "threat_source"
            },
            {
                "field": "ip_address"
            },
            {
                "field": "score"
            },
            {
                "field": "port"
            },
            {
                "field": "start_ts"
            },
            {
                "field": "end_ts"
            }
        ]
    },
    "reason": null,
    "result": "",
    "single_entry": true,
    "source_name": "threat_intelligence",
    "source_type": "ThreatIntelligence",
    "tid": ""
}
```

14.2 EnrichmentSource - List

Lists all enrichment sources.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/EnrichmentSource
```

Success Response

```
[
    {
        "active ": true,
        "delete_status ": " ",
        "id ": "59467646d8aaa41be49d158b ",
        "last_updated ": 0,
```

(continues on next page)

(continued from previous page)

```
    "plugin_info ": {
      "source_fields ": [
        {
          "field ": "domain "
        },
        {
          "field ": "url "
        },
        {
          "field ": "category "
        },
        {
          "field ": "type "
        },
        {
          "field ": "threat_source "
        },
        {
          "field ": "ip_address "
        },
        {
          "field ": "score "
        },
        {
          "field ": "port "
        },
        {
          "field ": "start_ts "
        },
        {
          "field ": "end_ts "
        }
      ]
    },
    "reason ": null,
    "result ": " ",
    "single_entry ": true,
    "source_name ": "threat_intelligence ",
    "source_type ": "ThreatIntelligence ",
    "tid ": " "
  },
  {
    "active ": true,
    "delete_status ": " ",
    "id ": "59b0ffa5d8aaa42bf93f9b4c ",
```

(continues on next page)

(continued from previous page)

```
        "last_updated ": 1504772009,
        "plugin_info ": {
            "charset ": "utf_8 ",
            "csv_file ": "/opt/immune/app_store/norm/enrichment/csv/smoke.csv ",
            "includes_header ": true,
            "source_fields ": [
                {
                    "field ": "MYCOUNT ",
                    "name ": "ext-gen2231 ",
                    "type ": "string "
                },
                {
                    "field ": "nepal ",
                    "name ": "ext-gen2232 ",
                    "type ": "string "
                }
            ],
            "source_name ": "smoke "
        },
        "reason ": null,
        "result ": "Updated ",
        "source_info ": {
            "id ": "108110b2c924449f75c62e3e562e76c3 ",
            "source_name ": "CSV "
        },
        "source_name ": "smoke ",
        "source_type ": "CSV ",
        "tid ": " "
    },
    {
        "source_info": {
            "source_name": "IPtoHost",
            "id": "8ae49468e5596c0a6ee2bcf8152e1cfb"
        },
        "plugin_info": {
            "event_field_name": "event_field1",
            "host_field_name": "hostField1",
            "source_name": "new_del"
        },
        "source_name": "new_del",
        "plugin_version": "3.0.0.7",
        "plugin_type": "enrichmentscript",
        "actions": {
            "search": false,
            "detail": false,
```

(continues on next page)

(continued from previous page)

```
        "delete": true
      },
      "source_type": "IPtoHost",
      "reason": "",
      "result": "Updated",
      "tid": "",
      "last_updated": 1516781073,
      "_id": "5a683d9bbcd4eb3793c62c63",
      "active": true,
      "delete_status": ""
    }
]
```

14.3 EnrichmentSource - RefreshList

Updates the enrichment source list.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/EnrichmentSource/
↪refreshlist
```

Request Example

```
{
    "data": {}
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

FIFTEEN

FILESYSTEMCOLLECTOR

15.1 FileSystemCollector - Create

Creates a FileSystem Collector.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/FileSystemCollector
```

Parameter

Field	Label in UI	Type	Description
charset	Charset	String	Existing LogPoint charset. Obtain the value of the required charset using Charsets - List API. . Mandatory Field
device_id	-	String	Existing Device id . Execute Devices - List API to list the available devices and use the value of the id parameter. Mandatory Field
excludes	Exclude Paths	[String]	Excluded path of the file. Optional Field
parser	Parser	String	Select a Parser for the collector. Execute Parsers - List API to list the available parsers and use the value of the name parameter. Mandatory Field
path	File Path	String	Starting Directory of the file. Mandatory Field

Continued on next page

Table 1 – continued from previous page

Field	Label in UI	Type	Description
processpolicy	Processing Policy	String	Select a Processing Policy for the collector. Execute ProcessingPolicy - List API to list the available parsers and use the value of the id parameter. . Mandatory Field

Request Example

```
{
  "data": {
    "charset": "utf_8",
    "device_id": "57724aacd8aaa40b569bcb1f",
    "excludes": [
      "/var/log/h*.log"
    ],
    "parser": "LineParser",
    "path": "/var/log/upstart/*",
    "processpolicy": "57724aacd8aaa40b569bcb1fasd"
  }
}
```

Success Response

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

15.2 FileSystemCollector - Edit

Edits a FileSystem Collector with given ID.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/FileSystemCollector/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
charset	Charset	String	Existing LogPoint charset. Obtain the value of the required charset using Charsets - List API. . Mandatory Field
excludes	Exclude Paths	[String]	Excluded path and can be empty. Optional Field
id	-	String	Existing FileSystemCollector id . Mandatory Field
parser	Parser	String	Select a Parser for the collector. Execute Parsers - List API to list the available parsers and use the value of the name parameter. Mandatory Field
path	File Path	String	Starting Directory and cannot be empty. Mandatory Field
processpolicy	Processing Policy	String	Select a Processing Policy for the collector. Execute ProcessingPolicy - List API to list the available parsers and use the value of the id parameter. Mandatory Field

Request Example

```
{
   "data": {
      "charset": "utf_8",
      "excludes": [
         "/var/log/h*.log"
      ],
      "parser": "LineParser",
      "path": "/var/log/upstart/*",
      "processpolicy": "57724aacd8aaa40b569bcb1fasd"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

15.3 FileSystemCollector - Trash

Deletes a FileSystem Collector with given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/FileSystemCollector/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing FileSystemCollector id . Mandatory Field

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

SIXTEEN

FTPCOLLECTORPLUGIN

16.1 FTPCollectorPlugin - Create

Creates an FTP Collector.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/FTPCollectorPlugin
```

Parameter

Field	Label in UI	Type	Description
charset	Charset	String	Existing LogPoint charset. Obtain the value of the required charset from Charsets - List API. Mandatory Field
device_id	-	String	Existing Device id . Obtain the value of the required device_id using Devices - List API. Optional Field
parser	Parser	String	Existing Parser name . Obtain the required parser name using Parsers - List API. Mandatory Field
password	Password	String	FTP Collector password . Mandatory Field
policy_id	-	String	Respective LCP policy ID. Obtain the value of the required policy_id using LogCollectionPolicies - List API. Optional Field

Continued on next page

Table 1 – continued from previous page

Field	Label in UI	Type	Description
processpolicy	Processing Policy	String	Existing Processing Policy id . Obtain the value of the required Processing Policy using ProcessingPolicy - List API. Mandatory Field
sourcename	Source Name	String	FTP Collector source name (Unique for that device). Mandatory Field
username	Username	String	FTP Collector username .(Unique for that device). Mandatory Field

Request Example

```
{
   "data": {
      "charset": "utf_8",
      "device_id": "57724aacd8aaa40b569bcb1f",
      "parser": "LineParser",
      "password": "password",
      "processpolicy": "59103b90854ff52c2506991f",
      "sourcename": "linuxBase",
      "username": "TestCollector"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

16.2 FTPCollectorPlugin - Edit

Edits an FTP Collector with given ID.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/FTPCollectorPlugin/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
charset	Charset	String	Existing LogPoint charset . Obtain the value of the required charset from Charsets - List API. Mandatory Field
id	-	String	FTPCollectorPlugin uuid . To obtain the FTP Collector uuid , execute Devices - List API if the collector was configured using device id or execute LogCollectionPolicies - List API if the collector was configured using log collection policy id . Mandatory Field
parser	Parser	String	Existing Parser name . Obtain the required parser name using Parsers - List API. Mandatory Field
password	Password	String	FTP Collector password . Mandatory Field
processpolicy	Processing Policy	String	Existing Processing Policy id . Obtain the value of the required Processing Policy id using ProcessingPolicy - List API. Mandatory Field
sourcename	Source Name	String	FTP Collector source name (Unique for that device). Mandatory Field
username	Username	String	FTP Collector username .(Unique for that device). Mandatory Field

Request Example

```
{
   "data": {
      "charset": "utf_8",
      "parser": "LineParser",
      "password": "password",
      "processpolicy": "59103b90854ff52c2506991f",
      "sourcename": "linuxBase",
      "username": "TestCollector"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

16.3 FTPCollectorPlugin - Trash

Deletes an FTP Collector with given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/FTPCollectorPlugin/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	FTPCollectorPlugin uuid . To obtain the FTP Collector uuid , execute Devices - List API if the collector was configured using device id or execute LogCollectionPolicies - List API if the collector was configured using log collection policy id . Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

SEVENTEEN

FTPFETCHERPLUGIN

17.1 FTPFetcherPlugin - Create

Create ftp fetcher

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/FTPFetcherPlugin
```

Parameter

Field	Label in UI	Type	Description
charset	Charset	String	Existing LogPoint charset . Obtain the value of the required charset from Charsets - List API . Mandatory Field
device_id	-	String	Existing Device id . Obtain the value of the required device_id using Devices - List API. Optional Field
interval	Fetch Interval (minutes)	int	Fetch interval in minutes. Mandatory Field
namepattern	Filename Pattern	String	Regex pattern for filename match or empty for all. Optional Field
oldlogs	Forward Old Logs	String	Check point to extract old logs or not - If check should be "on" (exact) any other value is considered as "off". Optional Field
parser	Parser	String	Pick one from the available parsers. Mandatory Field

Continued on next page

Table 1 – continued from previous page

Field	Label in UI	Type	Description
password	Password	String	Password of the FTP fetcher. Mandatory Field
policy_id	-	String	Respective LCP policy ID. Obtain the value of the required policy_id using LogCollectionPolicies - List API. Optional Field
port	Port	int	Access port number. Mandatory Field
processpolicy	Processing Policy	String	Existing Processing Policy id . Obtain the value of the required Processing Policy using ProcessingPolicy - List API . Mandatory Field
remotepath	Relative FilePath	String	Remotepath to the file directory. Optional Field
username	Username	String	Username of the FTP fetcher. Mandatory Field

Request Example

```
{
   "data": {
      "charset": "utf_8",
      "device_id": "57724aacd8aaa40b569bcb1f",
      "interval": 5,
      "namepattern": "*.pyc",
      "oldlogs": "on",
      "parser": "LineParser",
      "password": "password",
      "port": 5800,
      "processpolicy": "57724aacd8aaa40b569bcb1fasd",
      "remotepath": "/base/collection/",
      "username": "TestCollector"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

17.2 FTPFetcherPlugin - Edit

Edit ftp fetcher with given ID

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/FTPFetcherPlugin/{id}
```

Parameter

Field	Label in UI	Type	Description
charset	Charset	String	Existing LogPoint charset . Obtain the value of the required charset from Charsets - List API . Mandatory Field
id	-	String	UUID of the respective FTPFetcherPlugin. To obtain the FTP fetcher uuid , execute Devices - List API if the collector was configured using device id or execute LogCollectionPolicies - List API if the collector was configured using log collection policy id . Mandatory Field
interval	Fetch Interval (minutes)	int	Fetch interval in minutes. Mandatory Field
namepattern	Filename Pattern	String	Regex pattern for filename match or empty for all. Optional Field
oldlogs	Forward Old Logs	String	Check point to extract old logs or not - If check should be "on" (exact) any other value is considered as "off". Optional Field
parser	Parser	String	Pick one from the available parsers. Mandatory Field
password	Password	String	Password of the FTP fetcher. Mandatory Field
port	Port	int	Access port number. Mandatory Field

Continued on next page

Table 2 – continued from previous page

Field	Label in UI	Type	Description
processpolicy	Processing Policy	String	Existing Processing Policy id . Obtain the value of the required Processing Policy using ProcessingPolicy - List API . Mandatory Field
remotepath	Relative FilePath	String	Remotepath to the file directory. Optional Field
username	Username	String	Username of the FTP fetcher. Mandatory Field

Request Example

```
{
   "data": {
      "charset": "utf_8",
      "interval": 5,
      "namepattern": "*.pyc",
      "oldlogs": "on",
      "parser": "LineParser",
      "password": "password",
      "port": 5800,
      "processpolicy": "57724aacd8aaa40b569bcb1fasd",
      "remotepath": "/base/collection/",
      "username": "TestCollector"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

17.3 FTPFetcherPlugin - TestExisting

Test ftp fetcher with given ID

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/FTPFetcherPlugin/{id}/
↪testexistingftp
```

Parameter

Field	Label in UI	Type	Description
id	-	String	UUID of the respective FTPFetcherPlugin. Obtain the value of the required FTPFetcherPlugin uuid using Devices - List API. . Mandatory Field

Request Example

```
{
  "data": {}
}
```

Success Response

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

17.4 FTPFetcherPlugin - TestNew

Test newly created ftp fetcher

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/FTPFetcherPlugin/
↪testnewftp
```

Parameter

Field	Label in UI	Type	Description
device_id	-	String	Existing Device id . Obtain the value of the required device_id using DeviceGroups - List API. Mandatory Field
interval	Fetch Interval (minutes)	int	Fetch interval in minutes. Mandatory Field
namepattern	Filename Pattern	String	Regex pattern for filename match or empty for all. Optional Field

Continued on next page

Table 4 – continued from previous page

Field	Label in UI	Type	Description
oldlogs	Forward Old Logs	String	Check point to extract old logs or not - If check should be "on" (exact) any other value is considered as "off". Optional Field
password	Password	String	Password of the FTP fetcher. Mandatory Field
port	Port	int	Access port number. Mandatory Field
remotepath	Relative FilePath	String	Remotepath to the file directory. Optional Field
username	Username	String	Username of the FTP fetcher. Mandatory Field

Request Example

```
{
   "data": {
      "device_id": "57724aacd8aaa40b569bcb1f",
      "interval": 5,
      "namepattern": "*.pyc",
      "oldlogs": "on",
      "password": "password",
      "port": 5800,
      "remotepath": "/base/collection/",
      "username": "TestCollector"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

17.5 FTPFetcherPlugin - Trash

Delete ftp fetcher with given ID

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/FTPFetcherPlugin/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	UUID of the respective FTPFetcherPlugin. To obtain the FTP fetcher uuid , execute Devices - List API if the collector was configured using device id or execute LogCollectionPolicies - List API if the collector was configured using log collection policy id . Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

EIGHTEEN

HARDWAREKEY

18.1 Hardwarekey - List

Lists the hardware key of the given LogPoint

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Hardwarekey
```

Success Response

```
[
    {
        "hardware_key": "00059-8FD3E-2801F-43049-DC859-9F197-6BA5C"
    }
]
```

CHAPTER

NINETEEN

INCIDENTS

19.1 Incidents - Close

Closes the incident with the given id.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Incidents/{id}/close
```

Parameter

Field	Label in UI	Type	Description
id	-	String	The incident id to close. Mandatory Field
incident_user_id	-	String	ID of the user on whose behalf you want to close the incident. Use Users - FetchUsers to obtain value for this parameter. Mandatory Field

Request Example

```
{
   "data": {
      "incident_user_id": "5a466e9dd8aaa4748d3977c7"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

19.2 Incidents - Comment

Adds comment on the incident with the given id.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Incidents/{id}/
↪comment
```

Parameter

Field	Label in UI	Type	Description
comment	Comment	String	Comment for the incident. Mandatory Field
id	-	String	The incident id to comment on. Mandatory Field
incident_user_id	-	String	ID of the user on whose behalf you want to comment on the incident. Use Users - FetchUsers to obtain value for this parameter. Mandatory Field

Request Example

```
{
   "data": {
      "comment": "Newly Created Incident",
      "incident_user_id": "5a466e9dd8aaa4748d3977c7"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

19.3 Incidents - FetchIncidentData

Fetches all the logs of the incident of the given id.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Incidents/{id}/
↪fetchIncidentData
```

Parameter

Field	Label in UI	Type	Description
id	-	String	ID of the incident whose logs you want to fetch. Mandatory Field

Request Example

```
{
    "data": {}
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}/{data_node}-
↪Logs/fetchLogData"
}
```

19.4 Incidents - FetchIncidents

Fetches the incidents based on filter conditions.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Incidents/fetch
```

Parameter

Field	Label in UI	Type	Description
assigned_to_users	USERS	[String]	List of IDs of the users who are assigned the incident. Optional Field

Continued on next page

Table 4 – continued from previous page

Field	Label in UI	Type	Description
attack_category	ATTACK CATEGORY	[String]	List of attack categories. The API filters the incidents that match all the attack categories in the provided list. You can use the MitreAttack - FetchMitreAttacks API to fetch the details of the attack categories available in the Fabric-enabled LogPoint. Optional Field
attack_tag	ATTACK TAG	[String]	List of attack tags. The API filters the incidents that match all the attack tags in the provided list. You can use the MitreAttack - FetchMitreAttacks API to fetch the details of the attack tags available in the Fabric-enabled LogPoint. Optional Field
end_date	-	int	End Date in epoch. Mandatory only when start_date is present in the request. Optional Field
log_source	LOG SOURCES	[String]	List of log sources. The API filters the incidents that match all the log sources in the provided list. Optional Field
name	NAME (OR ID)	String	It can be name of the incident or ID of alertrule or ID of incident to fetch. It can be a regex. Optional Field
risk	RISK	[String]	List of the risk level of the Incident. Accepts values such as “low”, “medium”, “high” and “critical”. Optional Field
start_date	-	int	Start Date in epoch. Mandatory only when end_date is present in the request. Optional Field
status	STATUS	[String]	List of the status of the incident. Accepts values such as “resolved”, “unresolved” and “closed”. Optional Field

Continued on next page

Table 4 – continued from previous page

Field	Label in UI	Type	Description
type	TYPE	[String]	List of types from which incident is generated. Accepts values such as “alert”, “search” and “UEBA”. Optional Field

Request Example

```
{
   "data": {
      "assigned_to_users": [
         "574fceedd8aaa40740736302",
         "624fceedd8aaa40740736304"
      ],
      "attack_category": [
         "Defense Evasion",
         "Persistence"
      ],
      "attack_tag": [
         "Security Account Manager",
         "LSASS Memory"
      ],
      "end_date": 1568943700,
      "log_source": [
         "log123",
         "log233"
      ],
      "name": "MyIncident",
      "risk": [
         "critical",
         "high"
      ],
      "start_date": 1538793210,
      "status": [
         "resolved",
         "unresolved"
      ],
      "type": [
         "alert"
      ]
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}/{data_node}"
}
```

19.5 Incidents - GetIncidentData

List the contents of the incident data from given Incident.

Important: You should perform FetchIncidentData API request before GetIncidentData to get the updated incident data.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Incidents/
↪IncidentData/{id}
```

Parameter

Field	Label in UI	Type	Description
id		String	Existing Incident id .

Success Response

```
[
   {
      "action": "indexing speed",
      "col_ts": "2020/07/15 08:38:27",
      "col_type": "filesystem",
      "collected_at": "LogPoint",
      "device_ip": "127.0.0.1",
      "device_name": "localhost",
      "indexing_mps": "0",
      "log_ts": "2020/07/15 08:38:22",
      "logpoint_name": "LogPoint",
      "msg": "2020-07-15 08:38:22.00399 IndexSearcherBenchmarker; indexing speed;
↪service=indexsearcher__logpoint; number_of_indexed_logs=0; time=60 s; indexing_mps=0;
↪thread=Thread-2",
      "norm_id": "LogPoint",
      "number_of_indexed_logs": "0",
      "object": "IndexSearcherBenchmarker",
      "repo_name": "_logpoint",
      "service": "indexsearcher__logpoint",
```

(continues on next page)

(continued from previous page)

```
        "sig_id": "10537",
        "source_name": "/opt/immune/var/log/benchmarker/indexsearcher__logpoint.log",
        "thread": "Thread-2",
        "time": "60"
    },
    {
        "col_ts": "2020/07/15 08:38:27",
        "col_type": "filesystem",
        "collected_at": "LogPoint",
        "device_ip": "127.0.0.1",
        "device_name": "localhost",
        "log_ts": "2020/07/15 08:38:20",
        "logpoint_name": "LogPoint",
        "msg": "2020-07-15_08:38:20.75642 Wed Jul 15 08:38:20 2020 UDPv4 link remote:[AF_
↪INET]89.188.79.98:1193",
        "repo_name": "_logpoint",
        "source_name": "/opt/immune/var/log/service/support_con_client/current"
    }
]
```

19.6 Incidents - Reassign

Reassigns the incident with the given id to a new user.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Incidents/{id}/reassign
```

Parameter

Field	Label in UI	Type	Description
id	-	String	The incident id to reassign. Mandatory Field
incident_user_id	-	String	ID of the user on whose behalf you want to reassign the incident. Use Users - FetchUsers to obtain value for this parameter. Mandatory Field

Request Example

```
{
    "data": {
```

(continues on next page)

(continued from previous page)

```
        "incident_user_id": "5a466e9dd8aaa4748d3977c7"
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

19.7 Incidents - Reopen

Reopens the incident with the given id.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Incidents/{id}/reopen
```

Parameter

Field	Label in UI	Type	Description
id	-	String	The incident id to reopen. Mandatory Field
incident_user_id	-	String	ID of the user on whose behalf you want to reopen the incident. Use Users - FetchUsers to obtain value for this parameter. Mandatory Field

Request Example

```
{
    "data": {
        "incident_user_id": "5a466e9dd8aaa4748d3977c7"
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

19.8 Incidents - Resolve

Resolves the incident with the given id.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Incidents/{id}/resolve
```

Parameter

Field	Label in UI	Type	Description
id	-	String	The incident id to resolve. Mandatory Field
incident_user_id	-	String	ID of the user on whose behalf you want to resolve the incident. Use Users - FetchUsers to obtain value for this parameter. Mandatory Field

Request Example

```
{
   "data": {
      "incident_user_id": "5a466e9dd8aaa4748d3977c7"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

19.9 Incidents - SendForInvestigation

Manually trigger notifications for the incident with the given ID.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Incidents/{id}/
↪sendForInvestigation
```

Parameter

Field	Label in UI	Type	Description
id	-	String	ID of the incident. Use the Incidents - FetchIncidents API to obtain the value of this parameter. Mandatory Field
incident_user_id	-	String	ID of the user on whose behalf you want to trigger the incident notification. Use the Users - FetchUsers API to obtain value for this parameter. Mandatory Field

Request Example

```
{
   "data": {
      "incident_user_id": "5a466e9dd8aaa4748d3977c7"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

TWENTY

INCIDENTUSERGROUPS

20.1 IncidentUserGroups - Create

Creates a new incident user group in a Fabric-enabled LogPoint

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/IncidentUserGroups
```

Parameter

Field	Label in UI	Type	Description
selected_usergroups	Select User Groups	[String]	List of usergroup(s) to be added to Incident Usergroup. Mandatory Field

Request Example

```
{
    "data": {
        "selected_usergroups": [
            "5faa0b4ebba538fa29cc7b52"
        ]
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

20.2 IncidentUserGroups - FetchIncidentUserGroup

Fetches Incident User Groups List.

DEPRECATED ! *Will be removed in future version. Use <b>IncidentUserGroups - List</b> API instead.*

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/IncidentUserGroups/
↪fetch
```

Request Example

```
{
   "data": {}
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}/{data_node}"
}
```

20.3 IncidentUserGroups - Get

Fetches a Incident UserGroup with given ID.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/IncidentUserGroups/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	ID of the existing incident usergroup that you want to fetch.

Success Response

```
{
   "id": "4fd04565f39d16242ad557cb",
```

(continues on next page)

(continued from previous page)

```
    "name": "usergroup1",
    "tid": "",
    "user": "admin",
    "usergroup": "4fcf16418b3e5c5027f18dbb",
    "users": [
        "4fcf176789f54399b15ef23a",
        "4fcf17c189f54399b15ef240"
    ]
}
```

20.4 IncidentUserGroups - List

Lists all existing Incident UserGroups.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/IncidentUserGroups
```

Success Response

```
[
    {
        "id": "4fd04565f39d16242ad557cb",
        "name": "usergroup1",
        "tid": "",
        "user": "admin",
        "usergroup": "4fcf16418b3e5c5027f18dbb",
        "users": [
            "4fcf176789f54399b15ef23a",
            "4fcf17c189f54399b15ef240"
        ]
    }
]
```

20.5 IncidentUserGroups - Trash

Removes the incident user group with given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/IncidentUserGroups/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	ID of the existing incident user group that you want to delete. Mandatory Field

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

TWENTYONE

IPLOOKUP

21.1 IPLookup - Delete

Delete the IPLookup Table with given ID

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/IPLookup/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing IPLookup Table id. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/v1/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

21.2 IPLookup - Install

Install a given application

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/IPLookup/install
```

Parameter

Field	Label in UI	Type	Description
file_location	-	String	Location of the file to install. can be either 'private' or 'public'. Mandatory Field
file_name	File	String	Name of the csv file for IP Lookup. Mandatory Field
name	Name	String	Name of IPLookup table to be created. Mandatory Field

Request Example

```
{
   "data": {
      "file_location": "private",
      "file_name": "ip_lookup.csv",
      "name": "IP"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/v1/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

21.3 IPLookup - List

List all IPLookup tables

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/IPLookup
```

Success Response

```
[
   {
      "filepath": "/opt/immune/app_store/IPLookup/IP.csv",
      "id": "5a1fd6ffd8aaa41eeee5e5cd",
      "name": "IP",
      "tid": ""
   },
   {
      "filepath": "/opt/immune/app_store/IPLookup/IP5.csv",
```

(continues on next page)

(continued from previous page)

```
    "id": "5a20f85bd8aaa41eeee5e5d0",
    "name": "IP5",
    "tid": ""
  }
]
```

21.4 IPLookup - TrashPrivate

Delete the file with given name from private storage

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/IPLookup/{file_name}
```

Parameter

Field	Label in UI	Type	Description
file_name		String	File to be deleted. Mandatory Field

Success Response

```
{
  "status": "Success",
  "message": "IP1.csv successfully deleted"
}
```

21.5 IPLookup - TrashPublic

Delete the file with given name from public storage

DELETE

```
https://api-server-host-name/configapi/IPLookup/{file_name}
```

Parameter

Field	Label in UI	Type	Description
file_name		String	File to be deleted. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "IP1.csv successfully deleted"
}
```

21.6 IPLookup - Upload

Upload files to private storage

POST

```
https://api-server-host-name/configapi/{pool_UUID}/IPLookup/upload
```

Header

Field	Label in UI	Description
file_name		File name of the file.
Content-Type		application/octet-stream
replace_existing		Set the value of this parameter as ‘true’ to replace the existing file with the same name with the new file. Default value is ‘false’. Value can be ‘true’ or ‘false’. Optional field

Parameter

Field	Label in UI	Type	Description
file	-	[Object]	(csv) to be uploaded. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "IP1.csv successfully uploaded in private storage. "
}
```

21.7 IPLookup - UploadPublic

Upload files to public storage

POST

```
https://api-server-host-name/configapi/IPLookup/publicupload
```

Header

Field	Label in UI	Description
file_name		File name of the file.
Content-Type		application/octet-stream
replace_existing		Set the value of this parameter as 'true' to replace the existing file with the same name with the new file. Default value is 'false'. Value can be 'true' or 'false'. Optional field

Parameter

Field	Label in UI	Type	Description
file	-	[Object]	(csv) to be uploaded. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "IP1.csv successfully uploaded in public storage."
}
```

21.8 IPLookup - UploadsList

List all files in private storage

GET

```
https://api-server-host-name/configapi/{pool_UUID}/IPLookup/list
```

Success Response

```
[
   "test.csv"
]
```

21.9 IPLookup - UploadsListPublic

List all files in public storage

GET

```
https://api-server-host-name/configapi/IPLookup/list
```

Success Response

```
[
    "test.csv"
]
```

CHAPTER

TWENTYTWO

LDAPAUTHENTICATION

22.1 LDAPAuthentication - Activate

Activate LDAP Strategy.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LDAPAuthentication/
↪{id}/activate
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing LDAP Strategy id . Mandatory Field

Request Example

```
{
   "data": {}
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

22.2 LDAPAuthentication - Create

Adds new LDAP Strategy.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LDAPAuthentication
```

Parameter

Field	Label in UI	Type	Description
auth_param	Authenticate Using	String	Authentication parameter “uid” or “dn” or “sAMAccountName”. Mandatory Field
bind_dn	Bind DN	String	Bind Distinguished Named of LDAP. Mandatory Field
bind_dn_password	Password	String	Bind DN password. Mandatory Field
description	Description	String	Description of the LDAP Strategy. Optional Field
enable_paginated_search	Enable Paginated Search	String	Enable/Disable search pagination. “on” or “off” (exact). Mandatory Field
fullname	Fullname Template	String	Fullname template. Optional Field
group_base_dn	Group Base DN	String	Node under which the LDAP groups are present. Mandatory Field
group_filter	Filter	String	Group Filter. Mandatory Field
group_member_attribute	Group Mem Attr	String	Group Member Attribute in database. Mandatory Field
group_name_attr	Group Name Attr	String	Attribute of group name provided in the database. Mandatory Field
host	Host	String	LDAP Host IP. Mandatory Field
ldap_mapping	LDAP User/Group Mapping	String	Value should be “on” (exact)to enable _ mapping_group_member_attr _ parameter or _ mapping_member_group_attr parameter. Mandatory Field
mapping_group_member_attr	User contains group info	String	LDAP user contains group info mapping. Mandatory if ‘mapping_member_group_attr’ not present. Optional Field
mapping_member_group_attr	Group contains user info	String	LDAP group contains user info mapping. Mandatory if ‘mapping_group_member_attr’ not present. Optional Field

Continued on next page

Table 2 – continued from previous page

Field	Label in UI	Type	Description
member_group_attribute	Mem Group Attr	String	members belonging to a group. Mandatory Field
name	Name	String	Name of LDAP Strategy. Mandatory Field
no_ldap_connection_check		boolean	Do not check connection to ldap server. “true” (exact). Optional Field
port	Port	int	Port of the LDAP Server. Mandatory Field
ssl	SSL	String	Value should be “on” (exact) to enable SSL communication with the host. Optional Field
user_base_dn	User Base DN	String	User Base DN. Mandatory Field
user_filter	Filter	String	String to filter user results. Mandatory Field
user_name_attr	User Name Attr	String	User Name Attributes in database. Mandatory Field
username	Username Template	String	Template of the username. Optional Field
users_unique_field	Unique Field	String	Unique identifier of LDAP user. Optional Field

Request Example

```
{
  "data": {
    "auth_param": "uid",
    "bind_dn": "CN=Administrator,CN=Users,DC=kb,DC=logpoint,DC=local",
    "bind_dn_password": "Dummy_Password",
    "description": "some description",
    "enable_paginated_search": "on",
    "fullname": "{{FirstName}}{{LastName}}",
    "group_base_dn": "DC=kb,DC=logpoint,DC=local",
    "group_filter": "objectCategory=group",
    "group_member_attribute": "dn",
    "group_name_attr": "cn",
    "host": "192.168.2.77",
    "ldap_mapping": "on",
    "mapping_member_group_attr": "member",
    "member_group_attribute": "dn",
    "name": "LDAP1",
    "port": 389,
```

(continues on next page)

(continued from previous page)

```
        "user_base_dn": "DC=kb,DC=logpoint,DC=local",
        "user_filter": "objectCategory=user",
        "user_name_attr": "cn",
        "username": "{{displayName}}"
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

22.3 LDAPAuthentication - Deactivate

Deactivate LDAP Strategy.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LDAPAuthentication/
↪{id}/deactivate
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing LDAP Strategy id . Mandatory Field

Request Example

```
{
    "data": {}
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

22.4 LDAPAuthentication - Edit

Edits existing LDAP Strategy with given ID.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LDAPAuthentication/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
auth_param	Authenticate Using	String	Authentication parameter "uid" or "dn" or "sAMAccountName". Mandatory Field
bind_dn	Bind DN	String	Bind Distinguished Named of LDAP. Mandatory Field
bind_dn_password	Password	String	Bind DN password. Mandatory Field
description	Description	String	Description of the LDAP Strategy. Optional Field
enable_paginated_search	Enable Paginated Search	String	Enable paginated search. "on" or "off" (exact). Mandatory Field
fullname	Fullname Template	String	Fullname template. Optional Field
group_base_dn	Group Base DN	String	Node under which the LDAP groups are present. Mandatory Field
group_filter	Filter	String	Group Filter. Mandatory Field
group_member_attribute	Group Mem Attr	String	Group Member Attribute in database. Mandatory Field
group_name_attr	Group Name Attr	String	Attribute of group name provided in the database. Mandatory Field
host	Host	String	IP of the LDAP Host. Mandatory Field
id	-	String	ID of existing LDAP Strategy. Mandatory Field
ldap_mapping	LDAP User/Group Mapping	String	Exactly "on". Mandatory Field

Continued on next page

Table 4 – continued from previous page

Field	Label in UI	Type	Description
mapping_group_member_attr	User contains group info	String	LDAP user contains group info mapping. Mandatory if 'mapping_member_group_attr' not present. Optional Field
mapping_member_group_attr	Group contains user info	String	LDAP group contains user info mapping. Mandatory if 'mapping_group_member_attr' not present. Optional Field
member_group_attribute	Mem Group Attr	String	Members belonging to a group. Mandatory Field
name	Name	String	Name of LDAP Strategy. Mandatory Field
no_ldap_connection_check		boolean	Do not check connection to ldap server. "true" (exact). Optional Field
port	Port	int	LDAP Server port. Mandatory Field
ssl	SSL	String	Enable SSL. "on" (exact). Optional Field
user_base_dn	User Base DN	String	User Base DN. Mandatory Field
user_filter	Filter	String	String to filter user results. Mandatory Field
user_name_attr	User Name Attr	String	User Name Attributes in database. Mandatory Field
username	Username Template	String	Username template. Optional Field
users_unique_field	Unique Field	String	Unique identifier of LDAP user. Optional Field

Request Example

```
{
   "data": {
      "auth_param": "uid",
      "bind_dn": "CN=Administrator,CN=Users,DC=kb,DC=logpoint,DC=local",
      "bind_dn_password": "Dummy_Password",
      "description": "some description",
      "enable_paginated_search": "on",
      "fullname": "{{FirstName}}{{LastName}}",
      "group_base_dn": "DC=kb,DC=logpoint,DC=local",
      "group_filter": "objectCategory=group",
```

(continues on next page)

(continued from previous page)

```
        "group_member_attribute": "dn",
        "group_name_attr": "cn",
        "host": "192.168.2.77",
        "ldap_mapping": "on",
        "mapping_member_group_attr": "member",
        "member_group_attribute": "dn",
        "name": "LDAP1",
        "port": 389,
        "user_base_dn": "DC=kb,DC=logpoint,DC=local",
        "user_filter": "objectCategory=user",
        "user_name_attr": "cn",
        "username": "{{displayName}}"
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

22.5 LDAPAuthentication - Get

Get LDAP Strategy with given id.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LDAPAuthentication/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing LDAP strategy id .

Success Response

```
{
    "active": true,
    "auth_param": "uid",
    "bind_dn": "CN=logpoint,CN=Users,DC=test,DC=com",
    "description": "",
    "group_base_dn": "DC=test,DC=com",
```

(continues on next page)

(continued from previous page)

```
    "group_filter": "objectCategory=group",
    "group_member_attribute": "dn",
    "group_name_attribute": "cn",
    "host": "10.45.1.146",
    "id": "5aa8f49a3dad6c2afb42cb28",
    "mapping_group_member_attr": "memberOf",
    "mapping_member_group_attr": null,
    "member_group_attribute": "dn",
    "member_represent_attr": null,
    "name": "ldap",
    "pagination": true,
    "port": 389,
    "ssl": false,
    "template_settings": {
        "fullname": "",
        "username": ""
    },
    "tid": "",
    "use_dn_auth": false,
    "use_dn_group": false,
    "user": "admin",
    "user_base_dn": "DC=test,DC=com",
    "user_filter": "objectCategory=user",
    "user_group_mapping": [],
    "user_name_attribute": "cn"
}
```

22.6 LDAPAuthentication - GetLDAPGroup

Fetches LDAP Users Group with given id.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LDAPAuthentication/
↪LDAPUserGroups/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing LDAP Strategy id .

Success Response

```
{
    "groups": [
        {
            "dn": "CN=SQLServerMSSQLServerADHelperUser$WIN-4H62SDE5M6B,CN=Users,
↪DC=test,DC=com",
            "name": "SQLServerMSSQLServerADHelperUser$WIN-4H62SDE5M6B",
            "timezone": null,
            "usergroup": null
        },
        {
            "dn": "CN=SQLServer2005SQLBrowserUser$WIN-4H62SDE5M6B,CN=Users,DC=test,
↪DC=com",
            "name": "SQLServer2005SQLBrowserUser$WIN-4H62SDE5M6B",
            "timezone": null,
            "usergroup": null
        },
        {
            "dn": "CN=SQLServerMSSQLUser$WIN-4H62SDE5M6B$SQLEXPRESS,CN=Users,
↪DC=test,DC=com",
            "name": "SQLServerMSSQLUser$WIN-4H62SDE5M6B$SQLEXPRESS",
            "timezone": null,
            "usergroup": null
        },
        {
            "dn": "CN=SQLServerSQLAgentUser$WIN-4H62SDE5M6B$SQLEXPRESS,CN=Users,
↪DC=test,DC=com",
            "name": "SQLServerSQLAgentUser$WIN-4H62SDE5M6B$SQLEXPRESS",
            "timezone": null,
            "usergroup": null
        },
        {
            "dn": "CN=HelpLibraryUpdaters,CN=Users,DC=test,DC=com",
            "name": "HelpLibraryUpdaters",
            "timezone": null,
            "usergroup": null
        }
    ],
    "id": "5ae03710d8aaa428908f2b33"
}
```

22.7 LDAPAuthentication - List

Lists all LDAP Strategies.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LDAPAuthentication
```

Success Response

```
[
    {
        "active": true,
        "auth_param": "uid",
        "bind_dn": "CN=logpoint,CN=Users,DC=test,DC=com",
        "description": "",
        "group_base_dn": "DC=test,DC=com",
        "group_filter": "objectCategory=group",
        "group_member_attribute": "dn",
        "group_name_attribute": "cn",
        "host": "10.45.1.146",
        "id": "5aa8f49a3dad6c2afb42cb28",
        "mapping_group_member_attr": "memberOf",
        "mapping_member_group_attr": null,
        "member_group_attribute": "dn",
        "member_represent_attr": null,
        "name": "ldap",
        "pagination": true,
        "port": 389,
        "ssl": false,
        "template_settings": {
            "fullname": "",
            "username": ""
        },
        "tid": "",
        "use_dn_auth": false,
        "use_dn_group": false,
        "user": "admin",
        "user_base_dn": "DC=test,DC=com",
        "user_filter": "objectCategory=user",
        "user_group_mapping": [],
        "user_name_attribute": "cn"
    }
]
```

22.8 LDAPAuthentication - ListLDAPGroup

Fetches list of LDAP Users Group.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LDAPAuthentication/
↪LDAPUserGroups
```

Success Response

```
[
  {
     "groups": [
        {
          "dn": "CN=SQLServerMSSQLServerADHelperUser$WIN-4H62SDE5M6B,CN=Users,
↪DC=test,DC=com",
          "name": "SQLServerMSSQLServerADHelperUser$WIN-4H62SDE5M6B",
          "timezone": null,
          "usergroup": null
        },
        {
          "dn": "CN=SQLServer2005SQLBrowserUser$WIN-4H62SDE5M6B,CN=Users,DC=test,
↪DC=com",
          "name": "SQLServer2005SQLBrowserUser$WIN-4H62SDE5M6B",
          "timezone": null,
          "usergroup": null
        },
        {
          "dn": "CN=SQLServerMSSQLUser$WIN-4H62SDE5M6B$SQLEXPRESS,CN=Users,
↪DC=test,DC=com",
          "name": "SQLServerMSSQLUser$WIN-4H62SDE5M6B$SQLEXPRESS",
          "timezone": null,
          "usergroup": null
        }
     ],
     "id": "5acae545d8aaa4398c1fadc1"
  }
]
```

22.9 LDAPAuthentication - MapLDAPGroup

Maps LDAP Group to LogPoint Users Group.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LDAPAuthentication/
↪{id}/mapldapgroup
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing LDAP Strategy id . Mandatory Field
ldapgroup	LDAP Group Name	String	LDAP Group name. Mandatory Field
timezone	Timezone	String	Timezone. Mandatory Field
usergroup	LogPoint User Group	String	LogPoint User Group or “None”. Mandatory Field

Request Example

```
{
   "data": {
      "ldapgroup": "Administrators",
      "timezone": "UTC",
      "usergroup": "LogPoint Administrator"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

22.10 LDAPAuthentication - RefreshLDAPGroupList

Updates LDAP User Groups list.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LDAPAuthentication/
↪LDAPUserGroups/refreshlist
```

Request Example

```
{
   "data": {}
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

22.11 LDAPAuthentication - Trash

Deletes LDAP Strategy.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LDAPAuthentication/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing LDAP Strategy id . Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

TWENTYTHREE

LABELPACKAGES

23.1 LabelPackages - Activate

Activates a LabelPackage with given ID.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LabelPackages/{id}/
↪activate
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing LabelPackage ID. Mandatory Field

Request Example

```
{
    "data": {}
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

23.2 LabelPackages - Clone

Clones a LabelPackage with given ID.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LabelPackages/
↪clonePackage
```

Parameter

Field	Label in UI	Type	Description
clone_name	Choose New Names	String	Name of the label package after getting cloned. Each label package name must be unique, and the value of the name parameter can contain alphanumeric characters, hyphen (-), white space character, and underscore (_). It must begin and end with an alphanumeric character and the total length must be between 2 and 100 characters. It must not begin with **LP_**. Mandatory Field
package_id	-	String	Existing LabelPackage ID. Mandatory Field
replace	Replace Existing?	String	Value can be "on" or "off". Set value as "on"(exact) to replace an existing package with the same name. Optional Field

Request Example

```
{
   "data": {
      "clone_name": "mylabelpackage",
      "package_id": "57591a2cd8aaa41bfef54888",
      "replace": "on"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

23.3 LabelPackages - Create

Creates a new Label Package

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LabelPackages
```

Parameter

Field	Label in UI	Type	Description
description	Description	String	Description of the Label Package. Optional Field
name	Name	String	Name of the label package. Each label package name must be unique, and the value of the name parameter can contain alphanumeric characters, hyphen (-), white space character, and underscore (_). It must begin and end with an alphanumeric character and the total length must be between 2 and 100 characters. It must not begin with **LP_**. Mandatory Field

Request Example

```
{
   "data": {
      "description": "this is custom package",
      "name": "mylabelpackage"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

23.4 LabelPackages - Deactivate

Deactivates a LabelPackage with given ID.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LabelPackages/{id}/
↪deactivate
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing LabelPackage ID. Mandatory Field

Request Example

```
{
    "data": {}
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

23.5 LabelPackages - Edit

Edits the Label Package with given id

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LabelPackages/{id}
```

Parameter

Field	Label in UI	Type	Description
description	Description	String	Description of the Label Package. Optional Field
id	-	String	LabelPackage id. Mandatory Field

Continued on next page

Table 5 – continued from previous page

Field	Label in UI	Type	Description
name	Name	String	Name of the label package. Each label package name must be unique, and the value of the name parameter can contain alphanumeric characters, hyphen (-), white space character, and underscore (_). It must begin and end with an alphanumeric character and the total length must be between 2 and 100 characters. It must not begin with **LP_**. Mandatory Field

Request Example

```
{
  "data": {
    "description": "this is custom package",
    "name": "mylabelpackage"
  }
}
```

Success Response

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

23.6 LabelPackages - Get

Gets the LabelPackage with given ID.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LabelPackages/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	ID of the existing LabelPackage that you want to fetch.

Success Response

```
{
   "active": true,
   "description": "abc",
   "id": "5ff5536d6581a5a5aba953b6",
   "labels": [
      {
         "active": false,
         "id": "4bebdbadd8aaa44216bdfc32",
         "labels": [
            "Update",
            "Successful"
         ],
         "package_id": "5ff5536d6581a5a5aba953b6",
         "package_name": "LP_Trend Micro Control Manager ",
         "query": "norm_id=TrendMicroControlManager event_category=*UPDATE_SUCCESS*",
         "share_is": false,
         "tid": "",
         "user": "LogPoint",
         "vid": "SEARCHLABEL_22000"
      }
   ],
   "name": "abc",
   "sharing_policy": "private",
   "tid": "",
   "user": "admin",
   "version": null,
   "vid": ""
}
```

23.7 LabelPackages - Install

Install a given labelpackage pak file

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LabelPackages/install
```

Parameter

Field	Label in UI	Type	Description
file_location	-	String	Location of the file to install. Can be either 'private' or 'public'. Mandatory Field
file_name	Search Labels	String	Name of the pak file for LabelPackage. Mandatory Field

Request Example

```
{
   "data": {
      "file_location": "private",
      "file_name": "labelpackage.pak"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

23.8 LabelPackages - List

Lists all LabelPackages in the Fabric-enabled LogPoint.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LabelPackages
```

Success Response

```
[
   {
      "active": true,
      "description": "abc",
      "id": "5ff5536d6581a5a5aba953b6",
      "labels": [
         {
            "active": false,
            "id": "4bebdbadd8aaa44216bdfc32",
            "labels": [
               "Update",
               "Successful"
```

(continues on next page)

(continued from previous page)

```
                ],
                "package_id": "5ff5536d6581a5a5aba953b6",
                "package_name": "LP_Trend Micro Control Manager ",
                "query": "norm_id=TrendMicroControlManager event_category=*UPDATE_SUCCESS*
↪",
                "share_is": false,
                "tid": "",
                "user": "LogPoint",
                "vid": "SEARCHLABEL_22000"
            }
        ],
        "name": "abc",
        "sharing_policy": "private",
        "tid": "",
        "user": "admin",
        "version": null,
        "vid": ""
    }
]
```

23.9 LabelPackages - ListPrivateUploads

List all the pak files that contains labelpackages in private storage

GET

```
https://api-server-host-name/configapi/{pool_UUID}/LabelPackages/list
```

Success Response

```
[
    "LabelPackages.pak"
]
```

23.10 LabelPackages - ListPublicUploads

List all the pak files that contains labelpackages in public storage

GET

```
https://api-server-host-name/configapi/LabelPackages/list
```

Success Response

```
[
   "LabelPackages.pak"
]
```

23.11 LabelPackages - Trash

Removes the LabelPackage with given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LabelPackages/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	ID of the existing LabelPackage that you want to delete. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

23.12 LabelPackages - TrashPrivateUploads

Delete the file with given name from private storage

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/LabelPackages/{file_name}
```

Parameter

Field	Label in UI	Type	Description
file_name	-	String	Name of the file to be deleted. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "LabelPackages.pak successfully deleted"
}
```

23.13 LabelPackages - TrashPublicUploads

Delete the file with given name from public storage

DELETE

```
https://api-server-host-name/configapi/LabelPackages/{file_name}
```

Parameter

Field	Label in UI	Type	Description
file_name	-	String	Name of the file to be deleted. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "LabelPackages.pak successfully deleted"
}
```

23.14 LabelPackages - Upload

Upload pak file containing labelpackages to private storage.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/LabelPackages/upload
```

Header

Field	Label in UI	Description
file_name		Name of the file to be uploaded.
Content-Type		application/octet-stream
replace_existing		Set the value of this parameter as ‘true’ to replace the existing file with the same name with the new file. Default value is ‘false’. Value can be ‘true’ or ‘false’. Optional field

Parameter

Field	Label in UI	Type	Description
file	-	[Object]	(pak) to be uploaded. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "LabelPackages.pak successfully uploaded in private storage. "
}
```

23.15 LabelPackages - UploadPublic

Upload pak file containing labelpackages to private storage.

POST

```
https://api-server-host-name/configapi/LabelPackages/publicupload
```

Header

Field	Label in UI	Description
file_name		Name of the file to be uploaded.
Content-Type		application/octet-stream
replace_existing		Set the value of this parameter as ‘true’ to replace the existing file with the same name with the new file. Default value is ‘false’. Value can be ‘true’ or ‘false’. Optional field

Parameter

Field	Label in UI	Type	Description
file	-	[Object]	(pak) to be uploaded. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "LabelPackages.pak successfully uploaded in public storage."
}
```

CHAPTER

TWENTYFOUR

LISTS

24.1 Lists - CreateDynamic

Creates a collection of list that collects specific values from the events during the runtime and stores them for a limited or an unlimited period.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Lists/dynamic
```

Parameter

Field	Label in UI	Type	Description
agelimit_day	Day	int	Age Limit is the expiration time for the values in the list. Specify the value for the day. Mandatory Field.
agelimit_hour	Hour	int	Specify the value for the hour. Mandatory Field.
agelimit_minute	Minute	int	Specify the value for the minute. Mandatory Field.
d_name	Name	String	Specify the name for the list which is automatically represented in uppercase. The value can be alpha numeric characters with underscore(_) and the value should not begin or end with white space character, hyphen(-) and underscore(_).The value should contain at least 2 characters and at most 100 characters. Mandatory Field.

Request Example

```
{
   "data": {
      "agelimit_day": 0,
      "agelimit_hour": 0,
      "agelimit_minute": 30,
      "d_name": "DEVICE_IP_LIST"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

24.2 Lists - CreateStatic

Creates a collection of pre-defined values which can be used to search those values efficiently.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Lists/static
```

Parameter

Field	Label in UI	Type	Description
lists	List of Values	[String]	List of values for s_name. Mandatory Field.
s_name	Name	String	Specify the name for the list which is automatically represented in uppercase. The value can be alpha numeric characters with underscore(_) and the value should not begin or end with white space character, hyphen(-) and underscore(_).The value should contain at least 2 characters and at most 100 characters. Mandatory Field.

Request Example

```
{
   "data": {
      "lists": [
         "10.1.1.1",
         "10.2.2.2"
      ],
      "s_name": "IP_BLACKLIST"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

24.3 Lists - EditDynamic

Edits a collection of list that collects specific values from the events during the runtime and stores them for a limited or an unlimited period.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Lists/dynamic/{id}
```

Parameter

Field	Label in UI	Type	Description
agelimit_day	Day	int	Age Limit is the expiration time for the values in the list. Specify the value for the day. Mandatory Field.
agelimit_hour	Hour	int	Specify the value for the hour. Mandatory Field.
agelimit_minute	Minute	int	Specify the value for the minute. Mandatory Field.
id	-	String	Existing Lists id . Obtain the value of the required Lists id using Lists - List API. Mandatory Field.

Request Example

```
{
   "data": {
      "agelimit_day": 0,
      "agelimit_hour": 0,
      "agelimit_minute": 30
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

24.4 Lists - EditStatic

Edits a collection of pre-defined values which can be used to search those values efficiently.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Lists/static/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing Lists id . Obtain the value of the required Lists id using Lists - List API. Mandatory Field.
lists	List of Values	[String]	List of values for s_name. Mandatory Field.

Request Example

```
{
   "data": {
      "lists": [
         "10.1.1.1",
         "10.2.2.2"
      ]
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

24.5 Lists - Get

Get list with given ID.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Lists/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing list_id.

Success Response

```
{
   "name": "IP_BLACKLIST",
   "lists": [
      "10.1.1.1",
      "10.2.2.2"
   ],
   "user": "admin",
   "tid": "",
   "lists_vendor": [],
   "list_type": "static_list",
   "age_limit": 0,
   "last_updated": "",
   "active": true,
   "hidden": false,
   "vid": "",
   "id": "57591a2cd8aaa41bfef54888"
}
```

24.6 Lists - Install

Install a given .pak, .txt or .csv file containing lists.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Lists/install
```

Parameter

Field	Label in UI	Type	Description
file_location	-	String	Location of the file uploaded to install. Can be either 'private' or 'public'. Mandatory Field.
file_name	-	String	Name of the .pak, .csv or .txt file containing Lists. Mandatory Field.

Request Example

```
{
   "data": {
      "file_location": "private",
      "file_name": "lists.pak"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

24.7 Lists - List

Lists all lists

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Lists
```

Success Response

```
[
  {
      "name": "IP_BLACKLIST",
      "lists": [
         "10.1.1.1",
         "10.2.2.2"
      ],
```

(continues on next page)

(continued from previous page)

```
        "user": "admin",
        "tid": "",
        "lists_vendor": [],
        "list_type": "static_list",
        "age_limit": 0,
        "last_updated": "",
        "active": true,
        "hidden": false,
        "vid": "",
        "id": "57591a2cd8aaa41bfef54888"
    }

]
```

24.8 Lists - ListPrivateUploads

List all the .pak, .csv or.txt files that contain list in private storage

GET

```
https://api-server-host-name/configapi/{pool_UUID}/Lists/list
```

Success Response

```
[
    "lists.pak",
    "lists.csv",
    "lists.txt"
]
```

24.9 Lists - ListPublicUploads

List all the .pak, .csv or.txt files that contain lists in public storage

GET

```
https://api-server-host-name/configapi/Lists/list
```

Success Response

```
[
    "lists.pak",
    "lists.csv",
```

(continues on next page)

(continued from previous page)

```
    "lists.txt"
]
```

24.10 Lists - RefreshList

Syncs the current data of lists with LogPoint's lists.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Lists/refreshlist
```

Request Example

```
{
    "data": {}
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

24.11 Lists - Trash

Deletes list of given ID

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Lists/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	existing list_id. Mandatory Field.

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

24.12 Lists - TrashPrivateUploads

Delete the file with given name from private storage

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/Lists/{file_name}
```

Parameter

Field	Label in UI	Type	Description
file_name		String	Name of the file to be deleted. Mandatory Field.

Success Response

```
{
   "status": "Success",
   "message": "lists.pak successfully deleted"
}
```

24.13 Lists - TrashPublicUploads

Delete the file with given name from public storage

DELETE

```
https://api-server-host-name/configapi/Lists/{file_name}
```

Parameter

Field	Label in UI	Type	Description
file_name		String	Name of the file to be deleted. Mandatory Field.

Success Response

```
{
   "status": "Success",
   "message": "lists.pak successfully deleted"
}
```

24.14 Lists - Upload

Upload .pak, .csv or.txt file containing lists to private storage.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/Lists/upload
```

Header

Field	Label in UI	Description
file_name		Name of the file to be uploaded.
Content-Type		application/octet-stream
replace_existing		Set the value of this parameter as 'true' to replace the existing file with the same name with the new file. Default value is 'false'. Value can be 'true' or 'false'. Optional Field.

Parameter

Field	Label in UI	Type	Description
file		[Object]	(.pak, .csv or .txt file) to be uploaded. Mandatory Field.

Success Response

```
{
   "status": "Success",
   "message": "lists.pak successfully uploaded in private storage. "
}
```

24.15 Lists - UploadPublic

Upload .pak, .csv or .txt file containing lists to public storage.

POST

```
https://api-server-host-name/configapi/Lists/publicupload
```

Header

Field	Label in UI	Description
file_name		Name of the file to be uploaded.
Content-Type		application/octet-stream
replace_existing		Set the value of this parameter as 'true' to replace the existing file with the same name with the new file. Default value is 'false'. Value can be 'true' or 'false'. Optional Field.

Parameter

Field	Label in UI	Type	Description
file		[Object]	(.pak, .csv or .txt file) to be uploaded. Mandatory Field.

Success Response

```
{
   "status": "Success",
   "message": "lists.pak successfully uploaded in public storage."
}
```

CHAPTER

TWENTYFIVE

LOGCOLLECTIONPOLICIES

25.1 LogCollectionPolicies - Create

Add a new log collection policy

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LogCollectionPolicies
```

Parameter

Field	Label in UI	Type	Description
description	Description	String	Description for the log collection policy. Optional Field
name	Name	String	Name of the log collection policy. Valid unique string. Mandatory Field

Request Example

```
{
   "data": {
      "description": "Created from API",
      "name": "lcp1"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

25.2 LogCollectionPolicies - Edit

Edit a log collection policy with given ID

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LogCollectionPolicies/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
description	Description	String	Description for the log collection policy. Optional Field
id	-	String	Existing log collection policy id . Obtain the value of the required log collection policy id using LogCollectionPolicies-List API. Mandatory Field

Request Example

```
{
   "data": {
      "description": "Created from API"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

25.3 LogCollectionPolicies - Get

Get log collection policy by given ID

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LogCollectionPolicies/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	ID of the existing log collection policy that you want to fetch.

Success Response

```
{
   "active": true,
   "col_apps": [
      {
         "app": "FTPFetcher",
         "charset": "utf_8",
         "interval": "5",
         "namepattern": "*.pyc",
         "oldlogs": "on",
         "parser": "LineParser",
         "password": "8PEzHGOmgWSf/rs8ETgyC5xbuzYwhGc/AWZ477uUhZU=",
         "policy_id": "5bbf4095d8aaa4276a2c1255",
         "port": "5800",
         "processpolicy": "5ab9f74cd8aaa45ad3e31e42",
         "remotepath": "/base/collection/",
         "sid": "ftpf|lcp21:testcollector:5800:/base/collection/:*.pyc",
         "username": "TestCollector",
         "uuid": "73e30fc730cd4dc98b3f7e635b35eabf"
      }
   ],
   "description": "CreatedFromAPI",
   "id": "5bbf4095d8aaa4276a2c1255",
   "name": "lcp21",
   "tid": ""
}
```

25.4 LogCollectionPolicies - GetPlugins

Get plugins by given log collection policy ID

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LogCollectionPolicies/
↪{id}/plugins
```

Parameter

Field	Label in UI	Type	Description
id	-	String	ID of the existing log collection policy that you want to fetch.

Success Response

```
[
  {
    "CSRFToken": "cknHNJFOKZGrCfm",
    "LOGGEDINUSER": "admin",
    "app": "SnareCollector",
    "charset": "utf_8",
    "hasLCP": "0",
    "ips": "181.170.0.101",
    "normalizer": "None",
    "parser": "LineParser",
    "repo": "default",
    "requestType": "formsubmit",
    "sid": "snare|device-NewDevice_101"
  },
  {
    "CSRFToken": "cknHNJFOKZGrCfm",
    "LOGGEDINUSER": "admin",
    "app": "SyslogCollector",
    "charset": "utf_8",
    "hasLCP": "0",
    "ips": "181.170.0.101",
    "normalizer": "None",
    "parser": "SyslogParser",
    "proxy_condition": "None",
    "repo": "default",
    "requestType": "formsubmit",
    "sid": "syslog|device-NewDevice_101"
  }
]
```

25.5 LogCollectionPolicies - List

Lists all log collection policies in the Fabric-enabled LogPoint.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LogCollectionPolicies
```

Success Response

```
[
   {
      "active": true,
      "col_apps": [
         {
            "app": "FTPFetcher",
            "charset": "utf_8",
            "interval": "5",
            "namepattern": "*.pyc",
            "oldlogs": "on",
            "parser": "LineParser",
            "password": "8PEzHGOmgWSf/rs8ETgyC5xbuzYwhGc/AWZ477uUhZU=",
            "policy_id": "5bbf4095d8aaa4276a2c1255",
            "port": "5800",
            "processpolicy": "5ab9f74cd8aaa45ad3e31e42",
            "remotepath": "/base/collection/",
            "sid": "ftpf|lcp21:testcollector:5800:/base/collection/:*.pyc",
            "username": "TestCollector",
            "uuid": "73e30fc730cd4dc98b3f7e635b35eabf"
         }
      ],
      "description": "CreatedFromAPI",
      "id": "5bbf4095d8aaa4276a2c1255",
      "name": "lcp21",
      "tid": ""
   },
   {
      "active": true,
      "col_apps": [],
      "description": "",
      "id": "5bc09048d8aaa4285487f21d",
      "name": "lcp_test",
      "tid": ""
   }
]
```

25.6 LogCollectionPolicies - Trash

Delete a log collection policy of given ID

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LogCollectionPolicies/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	ID of the existing log collection policy that you want to delete. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

TWENTYSIX

LOGSOURCES

26.1 LogSources - Create

Creates a new log source.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LogSources
```

Parameters

Field	Label in UI	Type	Description
config	-	json	Configuration of log source. Go to Universal REST API for Director Console API for more information on the configuration parameters to create log source using Universal Rest API Fetcher. Mandatory Field.
dc_metadata	-	json	Information related to log source template created in the Director Console. Optional Field.
description	Description	String	Additional information or details about the log source. Optional Field.
documentation_link	Documentation Link	String	URL or hyperlink that points to external documentation or reference materials associated with that specific log source. Optional Field.

Continued on next page

Table 1 – continued from previous page

Field	Label in UI	Type	Description
files	-	json	A key-value pair. The key represents a unique identifier, and the value represents the filename. Optional Field
logo	Logo	String	Base64 encoded logo image. Optional Field.
name	Name	String	Name of the log source. Mandatory Field.
type	-	String	Type or category of the log-generating device, application, or system from which the log data originates. Mandatory Field.
vendor_name	Vendor Name	String	Name of vendor where the log data originates. Optional Field.

Request Example

```
{
    "data":{
        "name": "logsource_name",
        "type": "UniversalRestApi",
        "vendor_name": "",
        "logo": "",
        "description": "",
        "documentation_link": "",
        "files": {
            "key_name1": "file_name1",
            "key_name2": "file_name2"
        },
        "config": {
            "Source": {
                "name": "logsource_name",
                "base_url": "https://10.45.9.123",
                "request_timeout": 30,
                "retry_after": 10,
                "interval": 30,
                "charset": "utf_8"
            },
            "Connector": {
                "auth_type": "none",
                "custom_headers": [
                {
```

(continues on next page)

(continued from previous page)

```
                    "key": "id",
                    "value": "15"
                }
                ],
                "enforce_https": true,
                "enable_proxy": false,
                "protocol": "http"
            },
            "Endpoints": [
                {
                "endpoint_name": "getApps",
                "method": "get",
                "endpoint": "/apps",
                "endpoints_custom_headers": [],
                "query_params": [],
                "incremental_value_response_field": "event",
                "log_filter_params_dataformat": "iso",
                "log_filter_params_from_value": "2023-10-05 11:13:47",
                "id": "bbf30918-8605-4f1f-8d7c-93ce3489d57e"
                }
            ],
            "RoutingPolicy": {
                "routing_criterion": [],
                "catch_all": "_logpoint"
            },
            "NormalizationPolicy": {
                "normalizers": [
                {
                    "name": "ThycoticSecretServerCompiledNormalizer",
                    "type": "compiled"
                },
                {
                    "name": "JSONCompiledNormalizer",
                    "type": "compiled"
                }
                ]
            },
            "EnrichmentPolicy": "642beb329fab980b50e4bb7e"
        }
    }
}
```

Success Response

```
{
```

(continues on next page)

(continued from previous page)

```
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

26.2 LogSources - Edit

Edits the log source with given ID.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LogSources/{id}
```

Parameter

Field	Label in UI	Type	Description
config	-	json	Configuration of log source. Mandatory Field.
dc_metadata	-	json	Information related to log source template created in the Director Console. Optional Field.
description	Description	String	Additional information or details about the log source. Optional Field.
documentation_link	Documentation Link	String	URL or hyperlink that points to external documentation or reference materials associated with that specific log source. Optional Field.
files	-	json	A key-value pair, where the key represents a unique identifier, and the value represents the filename. Optional Field
id	-	String	Existing log source ID. Mandatory Field.
logo	Logo	String	Base64 encoded logo image. Optional Field.
name	Name	String	Name of log source. Mandatory Field.

Continued on next page

Table 2 – continued from previous page

Field	Label in UI	Type	Description
type	-	String	Type or category of the log-generating device, application, or system from which the log data originates. Mandatory Field.
vendor_name	Vendor Name	String	Name of vendor where the log data originates. Optional Field.

Request Example

```
{
  "data":{
    "name": "logsource_name",
    "type": "UniversalRestApi",
    "vendor_name": "",
    "logo": "",
    "description": "",
    "documentation_link": "",
    "files": {
      "key_name1": "file_name1",
      "key_name2": "file_name2"
    },
    "config": {
      "Source": {
        "name": "logsource_name",
        "base_url": "https://10.45.9.123",
        "request_timeout": 30,
        "retry_after": 10,
        "interval": 30,
        "charset": "utf_8"
      },
      "Connector": {
        "auth_type": "none",
        "custom_headers": [
        {
          "key": "id",
          "value": "15"
        }
        ],
        "enforce_https": true,
        "enable_proxy": false,
        "protocol": "http"
      },
      "Endpoints": [
```

(continues on next page)

(continued from previous page)

```
                {
                "endpoint_name": "getApps",
                "method": "get",
                "endpoint": "/apps",
                "endpoints_custom_headers": [],
                "query_params": [],
                "incremental_value_response_field": "event",
                "log_filter_params_dataformat": "iso",
                "log_filter_params_from_value": "2023-10-05 11:13:47",
                "id": "bbf30918-8605-4f1f-8d7c-93ce3489d57e"
                }
            ],
            "RoutingPolicy": {
                "routing_criterion": [],
                "catch_all": "_logpoint"
            },
            "NormalizationPolicy": {
                "normalizers": [
                {
                    "name": "ThycoticSecretServerCompiledNormalizer",
                    "type": "compiled"
                },
                {
                    "name": "JSONCompiledNormalizer",
                    "type": "compiled"
                }
                ]
            },
            "EnrichmentPolicy": "642beb329fab980b50e4bb7e"
        }
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

26.3 LogSources - Get

Fetches a log source with given ID.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LogSources/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	ID of the existing log source to fetch.

Success Response

```
{
    "name": "LogSource",
    "log_source_type": "UniversalRestApi",
    "vendor_name": "",
    "logo": "",
    "description": "",
    "documentation_link": "",
    "config": {
        "Source": {
            "name": "LogSource",
            "base_url": "https://10.45.9.123",
            "request_timeout": 30,
            "retry_after": 10,
            "interval": 30,
            "charset": "utf_8",
            "source_name": "06f148533e9ac62e268e91dd790a8cfb",
            "sid": "06f148533e9ac62e268e91dd790a8cfb|10.45.9.123",
            "identifier": null
        },
        "Connector": {
            "auth_type": "none",
            "custom_headers": [
                {
                    "key": "id",
                    "value": "15"
                }
            ],
            "enforce_https": true,
            "enable_proxy": false,
            "protocol": "http",
            "ip": "",
            "port": ""
        },
        "Endpoints": [
            {
                "endpoint_name": "getApps",
```

(continues on next page)

(continued from previous page)

```
                "method": "get",
                "endpoint": "apps",
                "endpoints_custom_headers": [],
                "query_params": [],
                "incremental_value_response_field": "event",
                "log_filter_params_dataformat": "iso",
                "log_filter_params_from_value": "2023-10-05 11:13:47",
                "id": "bbf30918-8605-4f1f-8d7c-93ce3489d57e",
                "fetch_status": "",
                "last_fetch_attempt": ""
            }
        ],
        "RoutingPolicy": "651e49ad911faf6e24139ca4",
        "NormalizationPolicy": "651e49ad911faf6e24139ca3",
        "EnrichmentPolicy": "642beb329fab980b50e4bb7e"
    },
    "user": "642be720fad1d2b4e61f9773",
    "dc_metadata": {},
    "template": null,
    "last_log_received": null,
    "id": "651e49ad911faf6e24139ca5"
}
```

26.4 LogSources - List

List all log sources.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LogSources
```

Success Response

```
[
    {
        "name": "LogSource",
        "log_source_type": "UniversalRestApi",
        "vendor_name": "",
        "logo": "",
        "description": "",
        "documentation_link": "",
        "config": {
            "Source": {
                "name": "LogSource",
```

(continues on next page)

(continued from previous page)

```
            "base_url": "https://10.45.9.123",
            "request_timeout": 30,
            "retry_after": 10,
            "interval": 30,
            "charset": "utf_8",
            "source_name": "06f148533e9ac62e268e91dd790a8cfb",
            "sid": "06f148533e9ac62e268e91dd790a8cfb|10.45.9.123",
            "identifier": null
        },
        "Connector": {
            "auth_type": "none",
            "custom_headers": [
                {
                    "key": "id",
                    "value": "15"
                }
            ],
            "enforce_https": true,
            "enable_proxy": false,
            "protocol": "http",
            "ip": "",
            "port": ""
        },
        "Endpoints": [
            {
                "endpoint_name": "getApps",
                "method": "get",
                "endpoint": "apps",
                "endpoints_custom_headers": [],
                "query_params": [],
                "incremental_value_response_field": "event",
                "log_filter_params_dataformat": "iso",
                "log_filter_params_from_value": "2023-10-05 11:13:47",
                "id": "bbf30918-8605-4f1f-8d7c-93ce3489d57e",
                "fetch_status": "",
                "last_fetch_attempt": ""
            }
        ],
        "RoutingPolicy": "651e49ad911faf6e24139ca4",
        "NormalizationPolicy": "651e49ad911faf6e24139ca3",
        "EnrichmentPolicy": "642beb329fab980b50e4bb7e"
    },
    "user": "642be720fad1d2b4e61f9773",
    "dc_metadata": {},
    "template": null,
```

(continues on next page)

(continued from previous page)

```
        "last_log_received": null,
        "id": "651e49ad911faf6e24139ca5"
    }
]
```

26.5 LogSources - ListLogSourceMetaData

Lists schema version of log source.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LogSources/
↪LogSourceMetaData
```

Success Response

```
[
    {
        "SyslogCollector": {
            "schema_version": 0
        }
    }
]
```

26.6 LogSources - RefreshList

Syncs the current log source list with Logpoint's log source list.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LogSources/refreshlist
```

Request Example

```
{
    "data": {}
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

26.7 LogSources - Trash

Deletes the log source with given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/LogSources/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	ID of the existing log source to delete. Mandatory Field.

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

26.8 LogSources - Upload

Upload the log source .pak files to private storage. This must be used to upload log sources only.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/LogSources/upload
```

Header

Field	Label in UI	Description
file_name		Name of the file to be uploaded.
Content-Type		application/octet-stream
replace_existing		Set the value of this parameter as 'true' to replace the existing file with the same name with the new file. Default value is 'false'. Value can be 'true' or 'false'. Optional field.

Parameter

Field	Label in UI	Type	Description
file		[Object]	.pak to be uploaded. Mandatory Field.

Success Response

```
{
   "status": "Success",
   "message": "logsources.pak successfully uploaded in private storage. "
}
```

CHAPTER

TWENTYSEVEN

MACHINEINFO

27.1 MachineInfo - List

Lists the version history of the patch installed in a Logpoint. Will also list the basic info about the Logpoint machine like its name, current version, machine type etc.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/MachineInfo
```

Success Response

```
{
   "director_mode": "fabric_only",
   "is_lite": false,
   "is_zfs_supported": true,
   "machine_name": "LogPoint",
   "machine_type": "DLP",
   "pool_name": "standalone_pool",
   "version": "7.0.0",
   "version_history": [
     {
        "description": "logpoint 6.0.0",
        "installed_at": 1501147629,
        "package_type": "iso",
        "version": "6.0.0"
     },
     {
        "description": "logpoint 7.0.0",
        "installed_at": null,
        "package_type": "patch",
        "version": "7.0.0"
     }
   ]
}
```

CHAPTER

TWENTYEIGHT

MACROS

28.1 Macros - Create

Creates a new macro in a Fabric-enabled LogPoint.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Macros
```

Parameter

Field	Label in UI	Type	Description
name	Name	String	Name for the macro. The field supports alpha-numeric and underscore (_) characters. Mandatory Field
query	Query	String	Complete and valid Query. Mandatory Field

Request Example

```
{
   "data": {
      "name": "admin_log",
      "query": "user=admin"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

28.2 Macros - Edit

Edits the macro with given ID.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Macros/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing Macro id . Obtain the value of the required Macro id using Macros - List API. Mandatory Field
name	Name	String	Name for the macro. The field supports alpha-numeric and underscore (_) characters. Mandatory Field
query	Query	String	Complete and valid Query. Mandatory Field

Request Example

```
{
   "data": {
      "name": "admin_log",
      "query": "user=admin"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

28.3 Macros - Get

Fetches the macros with given ID.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Macros/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	ID of the existing macros that you want to fetch.

Success Response

```
{
   "id": "4ffbe8018dc3ad85f8116940",
   "name": "admin_log",
   "query": "user=admin",
   "tid": "",
   "user": "admin"
}
```

28.4 Macros - Install

Install a given pak file containing macros

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Macros/install
```

Parameter

Field	Label in UI	Type	Description
file_location	-	String	Location of the file uploaded to install. Can be either 'private' or 'public'. Mandatory Field
file_name	Macros	String	Name of the pak file containing Macros. Mandatory Field

Request Example

```
{
   "data": {
      "file_location": "private",
      "file_name": "macros.pak"
   }
}
```

Success Response

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

28.5 Macros - List

Lists all macros in the Fabric-enabled LogPoint.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Macros
```

Success Response

```
[
  {
    "id": "4ffbe8018dc3ad85f8116940",
    "name": "admin_log",
    "query": "user=admin",
    "tid": "",
    "user": "admin"
  }
]
```

28.6 Macros - ListPrivateUploads

List all the pak files that contains macro configurations in private storage

GET

```
https://api-server-host-name/configapi/{pool_UUID}/Macros/list
```

Success Response

```
[
  "macros.pak"
]
```

28.7 Macros - ListPublicUploads

List all the pak files that contains macro configurations in public storage

GET

```
https://api-server-host-name/configapi/Macros/list
```

Success Response

```
[
   "macros.pak"
]
```

28.8 Macros - Trash

Removes the macros with given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Macros/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	ID of the existing macros that you want to delete. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

28.9 Macros - TrashPrivateUploads

Delete the file with given name from private storage

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/Macros/{file_name}
```

Parameter

Field	Label in UI	Type	Description
file_name	-	String	Name of the file to be deleted. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "macros.pak successfully deleted"
}
```

28.10 Macros - TrashPublicUploads

Delete the file with given name from public storage

DELETE

```
https://api-server-host-name/configapi/Macros/{file_name}
```

Parameter

Field	Label in UI	Type	Description
file_name	-	String	Name of the file to be deleted. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "macros.pak successfully deleted"
}
```

28.11 Macros - Upload

Upload pak files that contains macros to private storage. This upload should be used for macros only.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/Macros/upload
```

Header

Field	Label in UI	Description
file_name		Name of the file to be uploaded.
Content-Type		application/octet-stream
replace_existing		Set the value of this parameter as 'true' to replace the existing file with the same name with the new file. Default value is 'false'. Value can be 'true' or 'false'. Optional field

Parameter

Field	Label in UI	Type	Description
file	-	[Object]	(pak) to be uploaded. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "macros.pak successfully uploaded in private storage. "
}
```

28.12 Macros - UploadPublic

Upload pak files that contains macros to to public storage. This upload should be used for macros only.

POST

```
https://api-server-host-name/configapi/Macros/publicupload
```

Header

Field	Label in UI	Description
file_name		Name of the file to be uploaded.
Content-Type		application/octet-stream
replace_existing		Set the value of this parameter as 'true' to replace the existing file with the same name with the new file. Default value is 'false'. Value can be 'true' or 'false'. Optional field

Parameter

Field	Label in UI	Type	Description
file	-	[Object]	(pak) to be uploaded. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "macros.pak successfully uploaded in public storage."
}
```

CHAPTER

TWENTYNINE

MITREATTACKS

29.1 MitreAttacks - FetchMitreAttacks

Lists all existing Mitre Attacks.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/MitreAttacks/fetch
```

Request Example

```
{
   "data": {}
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}/{data_node}"
}
```

CHAPTER

THIRTY

NORMALIZATIONPOLICY

30.1 NormalizationPolicy - Create

Creates a new Normalization Policy.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/NormalizationPolicy
```

Parameter

Field	Label in UI	Type	Description
compiled_normalizer	Compiled Normalizer	String	Comma separated names of the compiled normalizers. Obtain the required compiled normalizer name using NormalizationPackage - ListCompiledNormalizers API. Optional Field
name	Policy Name	String	Name for the Normalization Policy. Mandatory Field
norm_packages	Normalization Packages	String	Comma separated norm_package ids. NormPack - list. Optional Field

Request Example

```
{
   "data": {
      "compiled_normalizer": "JSONCompiledNormalizer,WindowsXMLCompiledNormalizer",
      "name": "_test1",
      "norm_packages": "567cf5487b011d9e45bda3f0,567cf5487b011d9e45bda3f3,
↪567cf5487b011d9e45bda3f1"
   }
```

(continues on next page)

(continued from previous page)

```
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

30.2 NormalizationPolicy - Edit

Edits the Normalization Policy with given ID.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/NormalizationPolicy/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
compiled_normalizer	Compiled Normalizer	String	Comma separated names of compiled normalizers. Optional Field
id	-	String	Existing normalization policy id . Mandatory Field
norm_packages	Normalization Packages	String	Comma separated Normalization Package ID. Optional Field

Request Example

```
{
   "data": {
      "compiled_normalizer": "JSONCompiledNormalizer,WindowsXMLCompiledNormalizer",
      "norm_packages": "567cf5487b011d9e45bda3f0,567cf5487b011d9e45bda3f3,
↪567cf5487b011d9e45bda3f1"
   }
}
```

Success Response

```
{
   "status": "Success",
```

(continues on next page)

(continued from previous page)

```
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

30.3 NormalizationPolicy - Get

Fetches a Normalization Policy with given id .

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/NormalizationPolicy/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Normalization Policy id .

Success Response

```
{
    "active": true,
    "id": "590ff8e943fe06bbb6ddff7b",
    "name": "_LogPointAlerts",
    "normalization_packages": [
        "590ff8c1d8aaa47064d4f6fd"
    ],
    "ordered_signatures": [],
    "selected_signatures": [
        "sig_405000",
        "sig_405001"
    ],
    "tid": ""
}
```

30.4 NormalizationPolicy - List

Lists all Normalization Policies.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/NormalizationPolicy
```

Success Response

```
[
   {
      "active": true,
      "id": "590ff8e943fe06bbb6ddff7b",
      "name": "_LogPointAlerts",
      "normalization_packages": [
         "590ff8c1d8aaa47064d4f6fd"
      ],
      "ordered_signatures": [],
      "selected_signatures": [
         "sig_405000",
         "sig_405001"
      ],
      "tid": ""
   }
]
```

30.5 NormalizationPolicy - Trash

Deletes a Normalization Policy with given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/NormalizationPolicy/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Normalization Policy id . ID of the Normalization Policy. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

THIRTYONE

NORMALIZATIONPACKAGE

31.1 NormalizationPackage - AddSignature

Adds a new signature to the Normalization Package.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪NormalizationPackage/Signatures
```

Parameter

Field	Label in UI	Type	Description
package_id	-	String	ID of the normalization package. Mandatory Field
extra_key_value	Key Values	json	Add extra key value pair to the normalized log. Optional Field
replace_key_value	Replace Keys	json	Replace the name of the keys. Optional Field
pattern	Pattern	String	Pattern of the signature. Mandatory Field
example	Example	String	Example of the log to be matched with the newsignature parameter. Optional Field

Request Example

```
{
  "data": {
    "package_id": "574fceedd8aaa40740736302",
    "extra_key_value": {
      "label": "Sonic,Firewall,Notice",
      "norm_id": "SonicFirewall"
    },
```

(continues on next page)

(continued from previous page)

```
    "replace_key_value": {
      "label": "Sonic",
      "norm_id": "SonicFirewall"
    },
    "pattern": "user<user:word><action:all>from source<source_address:ip>",
    "example": "user Bob logged in from source 192.168.2.10"
  }
}
```

Success Response

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

31.2 NormalizationPackage - CheckPattern

Check if the pattern matches with the example

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪NormalizationPackage/checkPattern
```

Parameter

Field	Label in UI	Type	Description
pattern	Pattern	String	Pattern of the signature. Mandatory Field
example	Example	String	Example of the log. Mandatory Field

Request Example

```
{
  "data": {
    "pattern": "&lt;:all&gt;&lt;process:'kernel'&gt;&lt;:all&gt;&lt;object:'logging'&gt;&lt;:all&gt;
↪&lt;action:'stopped'&gt;",
    "example": "Jun 1 22:20:05 secserv kernel: Kernel logging (proc) stopped."
  }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

31.3 NormalizationPackage - ClonePackage

Clone the normalization package

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪NormalizationPackage/clonePackage
```

Parameter

Field	Label in UI	Type	Description
clone_name	CHOOSE NEW NAMES	String	Name of the package to be cloned. Mandatory Field
replace	Replace Existing?	String	Set value as "on"(exact) to replace an existing package with the same name. Optional Field
package_id	-	String	ID of the normalization package which should be cloned. Mandatory Field

Request Example

```
{
   "data": {
      "clone_name": "package_clone",
      "replace": "on",
      "package_id": "5bd56ce6d8aaa414dc86587d"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

31.4 NormalizationPackage - Create

Adds a new Normalization Package.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/NormalizationPackage
```

Parameter

Field	Label in UI	Type	Description
name	Name	String	Name of the Normalization Package. The value of the name field must be unique alphanumeric values with hyphen (-) and underscore (_) characters, and it must not begin or end with a white space character, hyphen (-) and an underscore (_) . The total length has to be between 2 and 100 characters. Mandatory Field
description	Description	String	Description of the normalization package. Optional Field

Request Example

```
{
   "data": {
      "name": "LP_LogPoint",
      "description": "LogPoint System"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

31.5 NormalizationPackage - Edit

Edits a Normalization Package with given ID

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪NormalizationPackage/{id}
```

Parameter

Field	Label in UI	Type	Description
description	Description	String	Description of the normalization package. Optional Field
unused_signatures	-	[Integer]	List of the signature id(s) to be unused. Optional Field
order	-	[Integer]	List of all signature id(s) in the desired order. Optional Field
id	-	String	Existing normalization package id . Mandatory Field

Request Example

```
{
   "data": {
      "description": "LogPoint System",
      "unused_signatures": [
         500004,
         500005,
         500006
      ],
      "order": [
         500009,
         500010,
         500011,
         500003
      ]
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

31.6 NormalizationPackage - EditSignature

Edit a signature of the given normalization package

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪NormalizationPackage/Signatures/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	int	ID of the signature. Mandatory Field
extra_key_value	Key Values	json	Add extra key value pair to the normalized log. Optional Field
replace_key_value	Replace Values	json	Replace the name of the field. Optional Field
pattern	Pattern	String	Pattern of the signature. Mandatory Field
example	Example	String	Example of the log. Optional Field

Request Example

```
{
   "data": {
      "extra_key_value": {
         "label": "Sonic,Firewall,Notice",
         "norm_id": "SonicFirewall"
      },
      "replace_key_value": {
         "label": "Sonic",
         "norm_id": "SonicFirewall"
      },
      "pattern": "user<user:word><action:all>from source<source_address:ip>",
      "example": "user Bob logged in from source 192.168.2.10"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

31.7 NormalizationPackage - Get

Fetches a Normalization Package with given ID.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪NormalizationPackage/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing normalization package id .

Success Response

```
{
    "signatures": [
        {
            "kb_version": [
                "2"
            ],
            "hash": "4bc60c361723ce6ba26249a3ecb822b9",
            "package_name": "LP_LogPointAlerts",
            "vid": "SIG_40002",
            "pattern": "&lt;process:'config'&gt;&lt;:all&gt;&lt;action:'loaded'&gt;&lt;object:'resource
↪data'&gt;from&lt;path:all_max&gt;/&lt;file:all_max&gt;",
            "extra_key_value": {
                "norm_id": "vShieldEdgeLoadBalancer",
                "label": "Resource,Load"
            },
            "which_norm_package": 80,
            "unused": true,
            "replace_key_value": {},
            "sig_id": 40002,
            "example": "<30>Mar 7 04:20:40 vShieldEdge config: INFO :: CONFIG_MGR :: loaded
↪resource data from /var/db/vre/vseld/vse_one/config_se.psf"
        }
    ],
    "name": "LP_LogPointAlerts",
    "vid": "NORMPACKAGE_771",
    "unused_signatures": [
        40010
    ],
    "last_sig_id": 405001,
```

(continues on next page)

(continued from previous page)

```
    "active": true,
    "version": 3,
    "share_is": false,
    "tid": "",
    "fields_info": [],
    "type": "vendor",
    "id": "594b8e0ed8aaa46207ac6309",
    "description": "LogPoint Alert Triggered Incident"
}
```

31.8 NormalizationPackage - Install

Install a given normalization package pak file

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪NormalizationPackage/install
```

Parameter

Field	Label in UI	Type	Description
file_name	Normalization Package	String	Name of the pak file for normalization package. Mandatory Field
file_location	-	String	Location of the file to install. Can be either 'private' or 'public'. Mandatory Field

Request Example

```
{
    "data": {
        "file_name": "normpackage_1.pak",
        "file_location": "private"
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

31.9 NormalizationPackage - List

Lists all Normalization Packages.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/NormalizationPackage
```

Success Response

```
[
    {
        "signatures": [
            {
                "kb_version": [
                    "2"
                ],
                "hash": "4bc60c361723ce6ba26249a3ecb822b9",
                "package_name": "LP_LogPointAlerts",
                "vid": "SIG_40002",
                "pattern": "&lt;process:'config'&gt;&lt;:all&gt;&lt;action:'loaded'&gt;&lt;object:
↪'resource data'&gt;from&lt;path:all_max&gt;/&lt;file:all_max&gt;",
                "extra_key_value": {
                    "norm_id": "vShieldEdgeLoadBalancer",
                    "label": "Resource,Load"
                },
                "which_norm_package": 80,
                "unused": true,
                "replace_key_value": {},
                "sig_id": 40002,
                "example": "<30>Mar 7 04:20:40 vShieldEdge config: INFO :: CONFIG_MGR ::
↪loaded resource data from /var/db/vre/vseld/vse_one/config_se.psf"
            }
        ],
        "name": "LP_LogPointAlerts",
        "vid": "NORMPACKAGE_771",
        "unused_signatures": [
            40010
        ],
        "last_sig_id": 405001,
        "active": true,
        "version": 3,
        "share_is": false,
        "tid": "",
        "fields_info": [],
        "type": "vendor",
        "id": "594b8e0ed8aaa46207ac6309",
```

(continues on next page)

(continued from previous page)

```
        "description": "LogPoint Alert Triggered Incident"
    },
    {
        "signatures": [
            {
                "kb_version": [
                    "2"
                ],
                "hash": "4bc60c361723ce6ba26249a3ecb822b9",
                "package_name": "LP_vShield Edge LoadBalancer",
                "vid": "SIG_40002",
                "pattern": "&lt;:all&gt;&lt;process:'kernel'&gt;&lt;:all&gt;&lt;object:'logging'&gt;&lt;
↪:all&gt;&lt;action:'stopped'&gt;",
                "extra_key_value": {
                    "norm_id": "vShieldEdgeLoadBalancer",
                    "label": "Resource,Load"
                },
                "which_norm_package": 82,
                "unused": false,
                "replace_key_value": {},
                "sig_id": 40010,
                "example": "Jun 1 22:20:05 secserv kernel: Kernel logging (proc) stopped."
            }
        ],
        "name": "LP_vShield Edge LoadBalancer",
        "vid": "NORMPACKAGE_761",
        "unused_signatures": [],
        "last_sig_id": 405010,
        "active": true,
        "version": 3,
        "share_is": false,
        "tid": "",
        "fields_info": [],
        "id": "694b8e0ed8aaa46227ac6309",
        "type": "vendor",
        "description": "Edge LoadBalancer"
    }
]
```

31.10 NormalizationPackage - ListCompiledNormalizers

Lists all Compiled Normalizers installed in the LogPoint

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪NormalizationPackage/CompiledNormalizers
```

Success Response

```
[
   {
      "version": "3.3.0",
      "name": "CheckPointOpsecCompiledNormalizer"
   },
   {
      "version": "3.3.0",
      "name": "CheckPointInfinityCompiledNormalizer"
   },
   {
      "version": "3.0.0.1",
      "name": "RubrikCompiledNormalizer"
   },
   {
      "version": "3.0.0.1",
      "name": "PaloAltoCompiledNormalizer"
   }
]
```

31.11 NormalizationPackage - ListPrivateUploads

List all the pak files that contains normalization package in private storage

GET

```
https://api-server-host-name/configapi/{pool_UUID}/NormalizationPackage/list
```

Success Response

```
[
   "normpackage_1.pak"
]
```

31.12 NormalizationPackage - ListPublicUploads

List all the pak files that contains normalization package in public storage

GET

```
https://api-server-host-name/configapi/NormalizationPackage/list
```

Success Response

```
[
    "normpackage_1.pak"
]
```

31.13 NormalizationPackage - RefreshCompiledNormalizersList

Updates the CompiledNormalizers list to ensure consistency with the updated compiled normalizers list in Logpoint.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪NormalizationPackage/CompiledNormalizers/refreshlist
```

Request Example

```
{
    "data": {}
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

31.14 NormalizationPackage - ReorderSignature

Reorder signatures of given normalization package

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪NormalizationPackage/{id}/reorderSignatures
```

Parameter

Field	Label in UI	Type	Description
id	ID	String	Existing Normalization Package id . Mandatory Field
order	-	[Integer]	List of all signatures id(s) in the desired order. Mandatory Field

Request Example

```
{
   "data": {
      "order": [
         500009,
         500010,
         500011,
         500003
      ]
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

31.15 NormalizationPackage - Trash

Deletes a Normalization Package with given ID

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪NormalizationPackage/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing normalization package id. Mandatory Field

Success Response

```
{
```

(continues on next page)

(continued from previous page)

```
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

31.16 NormalizationPackage - TrashPrivateUploads

Delete the file with given name from private storage

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/NormalizationPackage/{file_name}
```

Parameter

Field	Label in UI	Type	Description
file_name		String	Name of the file to be deleted. Mandatory Field

Success Response

```
{
    "status": "Success",
    "message": "normpackage_1.pak successfully deleted"
}
```

31.17 NormalizationPackage - TrashPublicUploads

Delete the file with given name from public storage

DELETE

```
https://api-server-host-name/configapi/NormalizationPackage/{file_name}
```

Parameter

Field	Label in UI	Type	Description
file_name		String	Name of the file to be deleted. Mandatory Field

Success Response

```
{
    "status": "Success",
    "message": "normpackage_1.pak successfully deleted"
}
```

31.18 NormalizationPackage - TrashSignature

Delete a signature with given ID

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪NormalizationPackage/Signatures/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	int	Existing signature id. Mandatory Field

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

31.19 NormalizationPackage - UnuseSignature

Unuse given signatures of given normalization package

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪NormalizationPackage/{id}/unuseSignatures
```

Parameter

Field	Label in UI	Type	Description
unused_signatures	-	[Integer]	List of the signature id(s) to be unused. Optional Field

Continued on next page

Table 14 – continued from previous page

Field	Label in UI	Type	Description
id	ID	String	Existing normalization package id. Mandatory Field

Request Example

```
{
   "data": {
      "unused_signatures": [
         500004,
         500005,
         500006
      ]
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

31.20 NormalizationPackage - Upload

Upload pak files that contains normalization package to private storage. This upload should be used for normalization package only.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/NormalizationPackage/upload
```

Header

Field	Label in UI	Description
file_name		Name of the file to be uploaded.
Content-Type		application/octet-stream
replace_existing		Set the value of this parameter as 'true' to replace the existing file with the same name with the new file. Default value is 'false'. Value can be 'true' or 'false'. Optional field

Parameter

Field	Label in UI	Type	Description
file	-	[Object]	(pak) to be uploaded. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "normpackage_1.pak successfully uploaded in private storage. "
}
```

31.21 NormalizationPackage - UploadPublic

Upload pak files that contains normalization package to to public storage. This upload should be used for normalization package only.

POST

```
https://api-server-host-name/configapi/NormalizationPackage/publicupload
```

Header

Field	Label in UI	Description
file_name		Name of the file to be uploaded.
Content-Type		application/octet-stream
replace_existing		Set the value of this parameter as 'true' to replace the existing file with the same name with the new file. Default value is 'false'. Value can be 'true' or 'false'. Optional field

Parameter

Field	Label in UI	Type	Description
file	-	[Object]	(pak) to be uploaded. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "normpackage_1.pak successfully uploaded in public storage."
}
```

CHAPTER

THIRTYTWO

OPENDOOR

32.1 OpenDoor - Create

Creates a new remote connection for a Distributed LogPoint setup (Distributed LogPoints and Distributed Collectors).

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/OpenDoor
```

Parameter

Field	Label in UI	Type	Description
netmask	Netmask	String	Netmask address of the Fabric-enabled LogPoint. Mandatory only when the value of opened parameter is set as "on". Optional Field
network	Private IP	String	Private ip address of the Fabric-enabled LogPoint. Mandatory only when value of opened parameter is set as "on". The last octet of the IP address should always be 1 (x.x.x.1). Optional Field
opened	Open Door	String	Set the value of this parameter as "on" to enable a remote connection. Requesting this endpoint with empty data will disable the remote connection. Optional Field

Continued on next page

Table 1 – continued from previous page

Field	Label in UI	Type	Description
password	Password	String	Password to establish a remote connection between individual LogPoints. Mandatory only when the value of opened parameter is set as “on”. Optional Field

Request Example

```
{
   "data": {
      "netmask": "255.255.255.0",
      "network": "10.4.0.1",
      "opened": "on",
      "password": "examplePassword"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

32.2 OpenDoor - Get

Lists the saved OpenDoor configuration with given open door id.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/OpenDoor/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	ID of open door

Success Response

```
{
   "id": "574fb123d8aaa4625bfe2d23",
   "mtu": 1500,
```

(continues on next page)

(continued from previous page)

```
    "netmask": "255.255.255.0",
    "network": "10.4.0.1",
    "opened": "on",
    "password": "5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8"
}
```

32.3 OpenDoor - List

Lists the saved OpenDoor configuration.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/OpenDoor
```

Success Response

```
[
    {
        "id": "574fb123d8aaa4625bfe2d23",
        "mtu": 1500,
        "netmask": "255.255.255.0",
        "network": "10.4.0.1",
        "opened": "on",
        "password": "5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8"
    }
]
```

32.4 OpenDoor - Save

Updates a new remote connection for a Distributed LogPoint setup (Distributed LogPoints and Distributed Collectors).

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/OpenDoor
```

Parameter

Field	Label in UI	Type	Description
mtu	MTU	int	Maximum Transmissions Unit (MTU) in bytes. All the packets transferred between the Main LogPoint and its Remote LogPoint(s) are chunked into the size of the specified MTU. The default value of the MTU is 1500. Optional Field
netmask	Netmask	String	Netmask address of the Fabric-enabled LogPoint. Mandatory only when the value of opened parameter is set as "on". Optional Field
network	Private IP	String	Private ip address of the Fabric-enabled LogPoint. Mandatory only when value of opened parameter is set as "on". The last octet of the IP address should always be 1 (x.x.x.1). Optional Field
opened	Open Door	String	Set the value of this parameter as "on" to enable a remote connection. Requesting this endpoint with empty data will disable the remote connection. Optional Field
password	Password	String	Password to establish a remote connection between individual LogPoints. Mandatory only when the value of opened parameter is set as "on". Optional Field

Request Example

```
{
    "data": {
        "mtu": 1500,
        "netmask": "255.255.255.0",
        "network": "10.4.0.1",
        "opened": "on",
        "password": "examplePassword"
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

THIRTYTHREE

PARSERS

33.1 Parsers - Check

Checks the regex pattern.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Parsers/check
```

Parameter

Field	Label in UI	Type	Description
example	Example	String	Sample value to match with the pattern parameter. Mandatory Field
name	Name	String	Name of parser. Mandatory Field
pattern	Pattern	String	Regex pattern. Mandatory Field

Request Example

```
{
  "data": {
    "example": "\"123\"",
    "name": "testName",
    "pattern": "\"[0-9]{3}\""
  }
}
```

Success Response

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

33.2 Parsers - Create

Creates a new Parser.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Parsers
```

Parameter

Field	Label in UI	Type	Description
example	Example	String	Sample value to match with the pattern parameter. Mandatory Field
name	Name	String	Name of the parser. Mandatory Field
pattern	Pattern	String	Regex pattern. Mandatory Field

Request Example

```
{
   "data": {
      "example": "\"123\"",
      "name": "testName",
      "pattern": "\"[0-9]{3}\""
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

33.3 Parsers - Edit

Edits a parser

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Parsers/{id}
```

Parameter

Field	Label in UI	Type	Description
example	Example	String	Sample value to match. Mandatory Field
id	-	String	Existing parser id . Mandatory Field
pattern	Pattern	String	Regex pattern. Mandatory Field

Request Example

```
{
   "data": {
      "example": "\"123\"",
      "pattern": "\"[0-9]{3}\""
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

33.4 Parsers - Get

Fetches a Parser with given ID.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Parsers/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing Parser id .

Success Response

```
{
   "_permission": {
      "delete": false,
      "edit": false
   },
   "active": true,
```

(continues on next page)

(continued from previous page)

```
    "id": "590ff83bd8aaa45bad0d9b0d",
    "name": "LineParser",
    "pattern": "",
    "tid": "",
    "type": "LineParser",
    "user": "LogPoint",
    "vid": "LineParser"
}
```

33.5 Parsers - List

Lists all Parsers.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Parsers
```

Success Response

```
[
    {
        "_permission": {
            "delete": false,
            "edit": false
        },
        "active": true,
        "id": "590ff83bd8aaa45bad0d9b0d",
        "name": "LineParser",
        "pattern": "",
        "tid": "",
        "type": "LineParser",
        "user": "LogPoint",
        "vid": "LineParser"
    },
    {
        "_permission": {
            "delete": true,
            "edit": true
        },
        "active": true,
        "example": "\"123\"",
        "id": "59156b65d8aaa42d2f2c72f7",
        "name": "Test6",
        "pattern": "\"[0-9]{3}\"",
```

(continues on next page)

(continued from previous page)

```
    "tid": "",
    "type": "RegexParser",
    "user": "admin",
    "vid": ""
  }
]
```

33.6 Parsers - Trash

Deletes a regex pattern with given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Parsers/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing parser id . Mandatory Field

Success Response

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

THIRTYFOUR

PERMISSIONGROUPS

34.1 PermissionGroups - Create

Creates a new permission group in a Fabric-enabled LogPoint.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/PermissionGroups
```

Parameter

Field	Label in UI	Type	Description
description	Description	String	Description of the permission group. Optional Field.
name	Name	String	Name of the permission group. The value of the name field must contain unique alphanumeric values that can include the hyphen (-) and underscore () characters. It must not begin or end with a white space character, hyphen (-) or an underscore () . The total length has to be between 2 and 100 characters. Mandatory Field.

Continued on next page

Table 1 – continued from previous page

Field	Label in UI	Type	Description
permissions	-	[json]	Permission items list. To define permissions, use the following parameters: **entity**: Permission item name. Can be either of the following: • Normalization Packages • Lists • Fields • Macros • Label Packages • Devices, DeviceGroups, Log Collection Policy and Parsers • Distributed Collectors • Processing Policy • Distributed LogPoints • Export Management • Raw Syslog Forwarder • SOAR Playbooks-Playbook Actions • SOAR Playbooks-Manage Playbook Triggers • SOAR Settings-Integrations • SOAR Settings-API Key • SOAR Settings-Licensing • SOAR Settings-My Products • SOAR Settings-Lists Management

Table 1 – continued from previous page

Field	Label in UI	Type	Description

Request Example

```
{
   "data": {
      "description": "Permission User",
      "name": "User",
      "permissions": [
         {
            "entity": "Devices, DeviceGroups, Log Collection Policy and Parsers",
            "permission": "READ"
         }
      ]
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

34.2 PermissionGroups - Edit

Edits an existing permission group in a Fabric-enabled LogPoint.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/PermissionGroups/{id}
```

Parameter

Field	Label in UI	Type	Description
description	Description	String	Description of the permission group. Optional Field.
id	-	String	Existing permission group id . Obtain the value of the required permission group id using PermissionGroups - List API. Mandatory Field.

Continued on next page

Table 2 – continued from previous page

Field	Label in UI	Type	Description
name	Name	String	Name of the permission group. The value of the name field must contain unique alphanumeric values that can include the hyphen (-) and underscore () characters. It must not begin or end with a white space character, hyphen (-) or an underscore () . The total length has to be between 2 and 100 characters. Mandatory Field.

Continued on next page

Table 2 – continued from previous page

Field	Label in UI	Type	Description
permissions	-	[json]	Permission items list. To define permissions, use the following parameters: **entity**: Permission item name. Can be either of the following: • Normalization Packages • Lists • Fields • Macros • Label Packages • Devices, DeviceGroups, Log Collection Policy and Parsers • Distributed Collectors • Processing Policy • Distributed LogPoints • Export Management • Raw Syslog Forwarder • SOAR Playbooks-Playbook Actions • SOAR Playbooks-Manage Playbook Triggers • SOAR Settings-Integrations • SOAR Settings-API Key • SOAR Settings-Licensing • SOAR Settings-My Products • SOAR Settings-Lists Management

Table 2 – continued from previous page

Field	Label in UI	Type	Description

Request Example

```
{
   "data": {
      "description": "Permission User",
      "name": "User",
      "permissions": [
         {
            "entity": "Devices, DeviceGroups, Log Collection Policy and Parsers",
            "permission": "READ"
         }
      ]
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

34.3 PermissionGroups - Get

Lists all existing Permission Groups.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/PermissionGroups/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	ID of the existing permission group that you want to fetch.

Success Response

```
{
   "name": "permissiongroupname",
   "description": "Test Permission Group",
   "tid": "",
```

(continues on next page)

(continued from previous page)

```
    "active": true,
    "permissions": [
      {
        "entity": "Normalization Packages",
        "permission": "DELETE"
      },
      {
        "entity": "Lists",
        "permission": "DELETE"
      },
      {
        "entity": "Fields",
        "permission": "DELETE"
      },
      {
        "entity": "Macros",
        "permission": "DELETE"
      },
      {
        "entity": "Label Packages",
        "permission": "DELETE"
      },
      {
        "entity": "Devices, DeviceGroups, Log Collection Policy and Parsers",
        "permission": "DELETE"
      },
      {
        "entity": "Distributed Collectors",
        "permission": "DELETE"
      },
      {
        "entity": "Processing Policy",
        "permission": "DELETE"
      },
      {
        "entity": "Distributed LogPoints",
        "permission": "DELETE"
      },
      {
        "entity": "Export Management",
        "permission": "DELETE"
      },
      {
        "entity": "Raw Syslog Forwarder",
        "permission": "NONE"
```

(continues on next page)

(continued from previous page)

```
        },
        {
            "entity": "SOAR Playbooks-Playbook Actions",
            "permission": "READ"
        },
        {
            "entity": "SOAR Playbooks-Manage Playbook Triggers",
            "permission": "DELETE"
        },
        {
            "entity": "SOAR Settings-Integrations",
            "permission": "DELETE"
        },
        {
            "entity": "SOAR Settings-API Key",
            "permission": "DELETE"
        },
        {
            "entity": "SOAR Settings-Licensing",
            "permission": "DELETE"
        },
        {
            "entity": "SOAR Settings-My Products",
            "permission": "DELETE"
        },
        {
            "entity": "SOAR Settings-Lists Management",
            "permission": "DELETE"
        },
        {
            "entity": "SOAR Settings-Import",
            "permission": "DELETE"
        },
        {
            "entity": "SOAR Settings-System Health",
            "permission": "DELETE"
        },
        {
            "entity": "SOAR Cases-Manage Cases",
            "permission": "CREATE_EDIT"
        }
    ],
    "id": "6311c733fe0249378c55bfa1"
}
```

34.4 PermissionGroups - List

Lists all existing Permission Groups.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/PermissionGroups
```

Success Response

```
[
    {
        "name": "permissiongroupname",
        "description": "Test Permission Group",
        "tid": "",
        "active": true,
        "permissions": [
            {
                "entity": "Normalization Packages",
                "permission": "DELETE"
            },
            {
                "entity": "Lists",
                "permission": "DELETE"
            },
            {
                "entity": "Fields",
                "permission": "DELETE"
            },
            {
                "entity": "Macros",
                "permission": "DELETE"
            },
            {
                "entity": "Label Packages",
                "permission": "DELETE"
            },
            {
                "entity": "Devices, DeviceGroups, Log Collection Policy and Parsers",
                "permission": "DELETE"
            },
            {
                "entity": "Distributed Collectors",
                "permission": "DELETE"
            },
            {
                "entity": "Processing Policy",
```

(continues on next page)

(continued from previous page)

```
            "permission": "DELETE"
        },
        {
            "entity": "Distributed LogPoints",
            "permission": "DELETE"
        },
        {
            "entity": "Export Management",
            "permission": "DELETE"
        },
        {
            "entity": "Raw Syslog Forwarder",
            "permission": "NONE"
        },
        {
            "entity": "SOAR Playbooks-Playbook Actions",
            "permission": "READ"
        },
        {
            "entity": "SOAR Playbooks-Manage Playbook Triggers",
            "permission": "DELETE"
        },
        {
            "entity": "SOAR Settings-Integrations",
            "permission": "DELETE"
        },
        {
            "entity": "SOAR Settings-API Key",
            "permission": "DELETE"
        },
        {
            "entity": "SOAR Settings-Licensing",
            "permission": "DELETE"
        },
        {
            "entity": "SOAR Settings-My Products",
            "permission": "DELETE"
        },
        {
            "entity": "SOAR Settings-Lists Management",
            "permission": "DELETE"
        },
        {
            "entity": "SOAR Settings-Import",
            "permission": "DELETE"
```

(continues on next page)

(continued from previous page)

```
        },
        {
            "entity": "SOAR Settings-System Health",
            "permission": "DELETE"
        },
        {
            "entity": "SOAR Cases-Manage Cases",
            "permission": "CREATE_EDIT"
        }
    ],
    "id": "6311c733fe0249378c55bfa1"
  }
]
```

34.5 PermissionGroups - Trash

Removes the permission group with the given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/PermissionGroups/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	ID of the existing permission group that you want to delete. Mandatory Field.

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

THIRTYFIVE

PLUGINCONFIGURATION

35.1 PluginConfiguration - Create

To configure plugin

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/PluginConfiguration/
↪{plugin_name}
```

Parameter

Field	Label in UI	Type	Description
data		Object	Plugin configuration in json format. Mandatory Field

Request Example

```
{
   "data": {
      "frequency": 5,
      "query": "device_name=localhost",
      "repo": "_logpoint"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/v1/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

35.2 PluginConfiguration - Edit

To update plugin configuration

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/PluginConfiguration/
↪{plugin_name}/{id}
```

Parameter

Field	Label in UI	Type	Description
data		Object	Plugin configuration in json format. Mandatory Field
id		String	Existing plugin configuration id. Mandatory Field

Request Example

```
{
   "data": {
      "frequency": 5,
      "query": "device_name=localhost",
      "repo": "_logpoint"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/v1/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

35.3 PluginConfiguration - EditInstall

Edit the install of the given file inside a plugin.

DEPRECATED ! *Use PluginConfiguration Edit API instead. Will be removed in future version.*

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/PluginConfiguration/
↪{plugin_name}/install/{id}
```

Parameter

Field	Label in UI	Type	Description
file_location		String	Location of the file to install. can be either 'private' or 'public'. Mandatory Field
id		String	Unique id. Mandatory Field

Request Example

```
{
   "data": {
      "file_location": "private",
      "files": {
         "file_key_1": "file_name_1.txt",
         "file_key_2": "file_name_2.crt"
      },
      "key2": "value2"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/v1/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

35.4 PluginConfiguration - Get

Get a plugin configurations by id

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/PluginConfiguration/
↪{collection}/{id}
```

Parameter

Field	Label in UI	Type	Description
id		String	Existing plugin configuration id

Success Response

```
[
  {
    "CSRFToken": "cknHNJFOKZGrCfm",
    "LOGGEDINUSER": "admin",
    "app": "SnareCollector",
    "charset": "utf_8",
    "hasLCP": "0",
    "ips": "181.170.0.101",
    "normalizer": "None",
    "parser": "LineParser",
    "repo": "default",
    "requestType": "formsubmit",
    "sid": "snare|device-NewDevice_101"
  }
]
```

35.5 PluginConfiguration - Install

Installs the given file inside a plugin.

DEPRECATED ! *Use PluginConfiguration Create API instead. Will be removed in future version.*

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/PluginConfiguration/
↪{plugin_name}/install
```

Parameter

Field	Label in UI	Type	Description
file_location		String	Location of the file to install. can be either 'private' or 'public'. Mandatory Field

Request Example

```
{
  "data": {
    "file_location": "private",
    "files": {
      "file_key_1": "file_name_1.txt",
      "file_key_2": "file_name_2.crt"
    },
    "key2": "value2"
```

(continues on next page)

(continued from previous page)

```
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/v1/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

35.6 PluginConfiguration - List

Get a plugin configurations

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/PluginConfiguration/
↪{collection}
```

Success Response

```
[
    {
        "CSRFToken": "cknHNJFOKZGrCfm",
        "LOGGEDINUSER": "admin",
        "app": "SnareCollector",
        "charset": "utf_8",
        "hasLCP": "0",
        "ips": "181.170.0.101",
        "normalizer": "None",
        "parser": "LineParser",
        "repo": "default",
        "requestType": "formsubmit",
        "sid": "snare|device-NewDevice_101"
    },
    {
        "CSRFToken": "cknHNJFOKZGrCfm",
        "LOGGEDINUSER": "admin",
        "app": "SyslogCollector",
        "charset": "utf_8",
        "hasLCP": "0",
        "ips": "181.170.0.101",
        "normalizer": "None",
        "parser": "SyslogParser",
```

(continues on next page)

(continued from previous page)

```
        "proxy_condition": "None",
        "repo": "default",
        "requestType": "formsubmit",
        "sid": "syslog|device-NewDevice_101"
    }
]
```

35.7 PluginConfiguration - ListPlugins

List all the pluggable plugins installed in the given logpoint

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/PluginConfiguration
```

Success Response

```
[
    {
        "id": "5bdaca3f20c20868893e8321",
        "name": "DirectorPOCFetcher",
        "type": "fetchers",
        "version": "3.0.1"
    }
]
```

35.8 PluginConfiguration - ListPrivateUploads

List all files in private storage for a plugin

GET

```
https://api-server-host-name/configapi/{pool_UUID}/PluginConfiguration/{plugin_name}/list
```

Success Response

```
[
    "test.pak"
]
```

35.9 PluginConfiguration - ListPublicUploads

List all files in public storage for a plugin

GET

```
https://api-server-host-name/configapi/PluginConfiguration/{plugin_name}/list
```

Success Response

```
[
    "test.pak"
]
```

35.10 PluginConfiguration - RefreshList

To sync plugin configuration collections

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/PluginConfiguration/
↪{plugin_name}/refreshlist
```

Parameter

Field	Label in UI	Type	Description
data		Object	Plugin configuration in json format. Mandatory Field

Request Example

```
{
    "data": {}
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/v1/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

35.11 PluginConfiguration - TestExisting

To test existing plugin configuration

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/PluginConfiguration/
↪{plugin_name}/{id}/testexisting
```

Parameter

Field	Label in UI	Type	Description
id		String	UUID of the respective Plugin. Mandatory Field

Request Example

```
{
   "data": {}
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/v1/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

35.12 PluginConfiguration - TestNew

To test plugin configuration

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/PluginConfiguration/
↪{plugin_name}/testnew
```

Parameter

Field	Label in UI	Type	Description
data		Object	Plugin configuration in json format. Mandatory Field

Request Example

```
{
   "data": {
      "frequency": 5,
      "query": "device_name=localhost",
      "repo": "_logpoint"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/v1/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

35.13 PluginConfiguration - Trash

Delete the plugin configuration with given ID

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/PluginConfiguration/
↪{plugin_name}/{id}?action={action}
```

Parameter

Field	Label in UI	Type	Description
action		String	Query string indicating special action for a plugin. Optional Field
id		String	Existing plugin configuration id. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/v1/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

35.14 PluginConfiguration - TrashPrivateUploads

Delete the file with given name from private storage for a plugin

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/PluginConfiguration/{plugin_name}/{file_
↪name}
```

Parameter

Field	Label in UI	Type	Description
file_name		String	File to be deleted. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "test1.pak successfully deleted from plugin's private storage."
}
```

35.15 PluginConfiguration - TrashPublicUploads

Delete the file with given name from public storage for a plugin

DELETE

```
https://api-server-host-name/configapi/PluginConfiguration/{plugin_name}/{file_name}
```

Parameter

Field	Label in UI	Type	Description
file_name		String	File to be deleted. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "test1.pak successfully deleted"
}
```

35.16 PluginConfiguration - Upload

Upload plugin specific files to private storage. Validation of maximum number of files and maximum size of each file done.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/PluginConfiguration/{plugin_name}/upload
```

Header

Field	Label in UI	Description
Content-Type		multipart/form-data
replace_existing		Set the value of this parameter as 'true' to replace the existing file with the same name with the new file. Default value is 'false'. Value can be 'true' or 'false'. Optional field

Parameter

Field	Label in UI	Type	Description
file_name		[Object]	File to be uploaded. There can be multiple instances of this parameter as per the plugin need. If same key is used multiple times in the same request, only a single key/value pair will be used. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "test.pak successfully uploaded in private storage. "
}
```

35.17 PluginConfiguration - UploadPublic

Upload plugin specific files to public storage. Validation of maximum number of files and maximum size of each file done.

POST

```
https://api-server-host-name/configapi/PluginConfiguration/{plugin_name}/publicupload
```

Header

Field	Label in UI	Description
Content-Type		multipart/form-data
replace_existing		Set the value of this parameter as 'true' to replace the existing file with the same name with the new file. Default value is 'false'. Value can be 'true' or 'false'. Optional field

Parameter

Field	Label in UI	Type	Description
file_name		[Object]	File to be uploaded. There can be multiple instances of this parameter as per the plugin need. If same key is used multiple times in the same request, only a single key/value pair will be used. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "test.pak successfully uploaded in public storage. "
}
```

CHAPTER

THIRTYSIX

PLUGINS

36.1 Plugins - Get

Fetches a Plugin with given ID.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Plugins/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing Plugin id .

Success Response

```
{
  "authentication": {
    "LDAPAuthentication": {
      "description": "Configure LDAP Strategies needed for LDAP Authentication",
      "manage": "App.pluggables.modules.Authentication.apps.LDAPAuthentication.Manage
↪",
      "name": "LDAPAuthentication",
      "preinstalled": true,
      "symlinks": "{}",
      "type": "authentication",
      "ui_text": "LDAP Authentication",
      "version": "1.0"
    }
  },
  "description": "This package contains all the default KB components and LogPoint plugins.",
  "errors": [],
  "fetchers": {
    "SnmpFetcher": {
      "description": "Configure Snmp Policies needed for adding Snmp Fetcher",
```

(continues on next page)

(continued from previous page)

```
        "manage": "App.pluggables.modules.Collection.apps.SNMPFetcher.Manage",
        "name": "SnmpFetcher",
        "no_config_generation": true,
        "preinstalled": true,
        "symlinks": "{}",
        "type": "fetchers",
        "ui_text": "Snmp Fetcher",
        "version": "1.0"
      }
    },
    "id": "592fe14ad8aaa408672de0e5",
    "knowledgebase": {
      "LogPoint": {
        "name": "LogPoint",
        "type": "knowledgebase",
        "version": "3.1.0"
      }
    },
    "name": "LogPoint",
    "not_deleteable": false,
    "older_versions": [],
    "plugins": {
      "MemoryNotification": {
        "enabled": true,
        "extra_info": {
          "interval": 60,
          "notification_type": "Memory Usage",
          "scheduling": true
        },
        "latest_version": "1.0",
        "type": "system_notification",
        "version": "1.0"
      }
    },
    "system_notification": {
      "CPUNotification": {
        "description": "Configure High CPU usage notifications",
        "extra_info": {
          "interval": 60,
          "notification_type": "CPU Usage",
          "scheduling": true
        },
        "manage": "App.pluggables.modules.SystemNotification.apps.CPUNotification.Manage
↪",
        "name": "CPUNotification",
```

(continues on next page)

(continued from previous page)

```
            "preinstalled": true,
            "symlinks": "{}",
            "type": "system_notification",
            "ui_text": "CPU Notification",
            "version": "1.0"
        },
        "DiskNotification": {
            "description": "Configure High Disk usage notifications",
            "extra_info": {
                "interval": 3600,
                "notification_type": "Disk Usage",
                "scheduling": true
            },
            "manage": "App.pluggables.modules.SystemNotification.apps.DiskNotification.Manage
↪",
            "name": "DiskNotification",
            "preinstalled": true,
            "symlinks": "{}",
            "type": "system_notification",
            "ui_text": "Disk Notification",
            "version": "1.0"
        },
        "MemoryNotification": {
            "description": "Configure High Memory usage notifications",
            "extra_info": {
                "interval": 60,
                "notification_type": "Memory Usage",
                "scheduling": true
            },
            "manage": "App.pluggables.modules.SystemNotification.apps.MemoryNotification.
↪Manage",
            "name": "MemoryNotification",
            "preinstalled": true,
            "symlinks": "{}",
            "type": "system_notification",
            "ui_text": "Memory Notification",
            "version": "1.0"
        }
    },
    "tid": "",
    "version": "3.1.0"
}
```

36.2 Plugins - List

Lists all the Plugins.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Plugins
```

Success Response

```
[
    {
        "description": "This package contains pluggable CSVEnrichmentSource.",
        "enrichmentsource": {
            "CSVEnrichmentSource": {
                "config_gen_script": "CSVEnrichmentSourceCfgGen.py",
                "extra_fields_in_sid": [],
                "manage": "",
                "name": "CSVEnrichmentSource",
                "no_config_generation": false,
                "no_config_generation_lite": true,
                "post_install": "post_install.sh",
                "pre_install": "",
                "service_name": "csvenrichmentsource",
                "service_run_script": "csvenrichmentsource/CSVEnrichmentSource.py",
                "symlinks": "{\"/opt/immune/app_store/col/pluggable/CSVEnrichmentSource/
↪webserver/CSV\"}",
                "type": "enrichmentsource",
                "ui": "ui/CSV",
                "ui_text": "CSVEnrichmentSource",
                "uninstall_script": "uninstall.sh",
                "version": "3.0.0.10",
                "webserver": "webserver/CSV"
            }
        },
        "errors": [],
        "id": "592fe11dd8aaa47ce69717a8",
        "name": "CSVEnrichmentSource",
        "not_deleteable": false,
        "older_versions": [],
        "plugins": {
            "CSVEnrichmentSource": {
                "enabled": true,
                "extra_info": {},
                "latest_version": "3.0.0.10",
                "type": "enrichmentsource",
                "version": "3.0.0.10"
```

(continues on next page)

(continued from previous page)

```
            }
        },
        "tid": "",
        "version": "3.0.0.10"
    }
]
```

36.3 Plugins - ListPluginsVersion

Lists all Plugins versions.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Plugins/PluginInfo
```

Success Response

```
[
    {
        "id": "5b4835e73c4eaa7fb08064fd",
        "name": "DirectorPOCFetcher",
        "type": "fetchers",
        "version": "3.0.1"
    }
]
```

36.4 Plugins - Uninstall

Uninstalls the Plugin with given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Plugins/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing Plugin id . Mandatory Field

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

THIRTYSEVEN

PROCESSINGPOLICY

37.1 ProcessingPolicy - Create

Adds a new Processing Policy.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/ProcessingPolicy
```

Parameter

Field	Label in UI	Type	Description
enrich_policy	Enrichment Policy	String	Existing Enrichment Policy id or None(exact). Use the value of the id parameter from EnrichmentPolicy - List API to obtain Enrichment Policy id . Mandatory Field
norm_policy	Normalization Policy	String	Existing Normalization Policy name or None(exact). Use the value of the name parameter from NormalizationPolicy - List API to obtain the value of Normalization Policy name . Mandatory Field
policy_name	Policy Name	String	Processing Policy name . Mandatory Field
routing_policy	Routing Policy	String	Existing Routing Policy id or None (exact). Use the value of the id parameter from RoutingPolicy - List API to obtain Routing Policy id . Mandatory Field

Request Example

```
{
  "data": {
    "enrich_policy": "57591a2cd8aaa41bfef54888",
    "norm_policy": "_logpoint",
    "policy_name": "policyName",
    "routing_policy": "586cc3edd8aaa406f6fdc8e3"
  }
}
```

Success Response

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

37.2 ProcessingPolicy - Edit

Edits the Processing Policy with given ID.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/ProcessingPolicy/{id}
```

Parameter

Field	Label in UI	Type	Description
enrich_policy	Enrichment Policy	String	Existing Enrichment Policy id or None(exact). Use the value of the id parameter from EnrichmentPolicy - List API to obtain Enrichment Policy id . Mandatory Field
id	-	String	Existing Processing Policy id . Mandatory Field
norm_policy	Normalization Policy	String	Existing Normalization Policy name or None(exact). Use the value of the name parameter from NormalizationPolicy - List API to obtain the value of Normalization Policy name . Mandatory Field
policy_name	Policy Name	String	Processing Policy name . Mandatory Field

Continued on next page

Table 2 – continued from previous page

Field	Label in UI	Type	Description
routing_policy	Routing Policy	String	Existing Routing Policy id or None (exact). Use the value of the id parameter from RoutingPolicy - List API to obtain Routing Policy id . Mandatory Field

Request Example

```
{
  "data": {
    "enrich_policy": "57591a2cd8aaa41bfef54888",
    "norm_policy": "_logpoint",
    "policy_name": "policyName",
    "routing_policy": "586cc3edd8aaa406f6fdc8e3"
  }
}
```

Success Response

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

37.3 ProcessingPolicy - Get

Fetches the Processing Policy with given ID.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/ProcessingPolicy/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing Processing Policy id . Use the value of the id parameter of the required Processing Policy from ProcessingPolicy - List API.

Success Response

```
{
    "active": true,
    "enrich_policy": "None",
    "id": "59099afa854ff52b6819a739",
    "norm_policy": "None",
    "policy_name": "test_processingpolicy7",
    "routing_policy": "590961d2d8aaa45aa5501ce2",
    "tid": ""
}
```

37.4 ProcessingPolicy - List

Lists all Processing Policies.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/ProcessingPolicy
```

Success Response

```
[
    {
        "active": true,
        "enrich_policy": "None",
        "id": "590961d2d8aaa45aa5501cdf",
        "norm_policy": "_logpoint",
        "policy_name": "_logpoint",
        "routing_policy": "590961d2d8aaa45aa5501cdd",
        "tid": ""
    },
    {
        "active": true,
        "enrich_policy": "57591a2cd8aaa41bfef54888",
        "id": "590961d2d8aaa45aa5501ce0",
        "norm_policy": "None",
        "policy_name": "default",
        "routing_policy": "590961d2d8aaa45aa5501cde",
        "tid": ""
    }
]
```

37.5 ProcessingPolicy - Trash

Deletes the Processing Policy with given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/ProcessingPolicy/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing Processing Policy id . Use the value of the id parameter of the Processing Policy to be deleted from ProcessingPolicy - List API. Mandatory Field

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

THIRTYEIGHT

QUERY

38.1 Query - ValidateLabelQuery

Validates the given query for Search Label.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Query/
↪validateLabelQuery
```

Parameter

Field	Label in UI	Type	Description
query	Query	String	Query to validate. Mandatory Field

Request Example

```
{
   "data": {
      "query": "user=john"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

38.2 Query - ValidateQuery

Validates the given query.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Query/validate
```

Parameter

Field	Label in UI	Type	Description
query	Query	String	Query to validate. Mandatory Field

Request Example

```
{
   "data": {
      "query": "user=john"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

THIRTYNINE

RAWSYSLOGFORWARDER

39.1 RawSyslogForwarder - Create

Creates a new Raw Syslog Forwarder

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/RawSyslogForwarder
```

Parameter

Field	Label in UI	Type	Description
device_config	-	[json]	Json containing information of the devices. LogPoint collects and forwards the raw syslog messages from the devices. Either can be absent or following parameters must be provided to define device_config. device_group : Id of devicegroup. Value should be an empty string when no device_group is present for the devices. Mandatory field. include_all_devices : Can be either true or false . devices should not be present in the request when include_all_devices is true. Optional field devices : list of devices. devices should be present and non empty when include_all_devices is either not present or false. Value should be present when device_group is empty. . Optional Field
pattern	Pattern	String	Provide the regex Pattern. Only the logs matching the specified pattern are forwarded.For example:’[0-9]+:’ forwards log only if any digit is present in logs. Optional Field
remote_syslog_collectors	Remote Target	[String]	ID of the Targets where the logs are to be forwarded. Mandatory Field

Request Example

```
{
   "data": {
      "device_config": [
         {
            "device_group": "60a4a72c2d76c9046d54a3b6",
            "include_all_devices": true
         },
         {
            "device_group": "40a4a72d2d76c9045d54a3b5",
```

(continues on next page)

(continued from previous page)

```
                "devices": [
                    "2344a72d2d76c9045d54a3c6",
                    "5674a72d2d76c9045d54a3d7"
                ]
            }
        ],
        "pattern": "[0-9]+",
        "remote_syslog_collectors": [
            "60a4a72c2d76c9046d54a3b6",
            "31a4a72c2e66c9046d54a3c2"
        ]
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

39.2 RawSyslogForwarder - CreateTarget

Creates a new Target

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/RawSyslogForwarder/
↪Target
```

Parameter

Field	Label in UI	Type	Description
enable_udp	Protocol	String	Accepts either "on" or "off" values only. "on" implies UDP while "off" implies TCP being selected as protocol for sending syslogmessage. Mandatory Field
ip	IP	String	Ip address or hostname of the target device. Mandatory Field
name	Name	String	Name of the target. Mandatory Field

Continued on next page

Table 2 – continued from previous page

Field	Label in UI	Type	Description
port	Port	int	Port number for the input port of the target. Mandatory Field

Request Example

```
{
   "data": {
      "enable_udp": "on",
      "ip": "10.45.6.15",
      "name": "target_1",
      "port": 514
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

39.3 RawSyslogForwarder - Edit

Updates the existing configuration of the Raw Syslog Forwarder with the given id.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/RawSyslogForwarder/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
device_config	-	[json]	Json containing information of the devices. LogPoint collects and forwards the raw syslog messages from the devices. Either can be absent or following parameters must be provided to define device_config. device_group : Id of devicegroup. Value should be an empty string when no device_group is present for the devices. Mandatory field. include_all_devices : Can be either true or false . devices should not be present in the request when include_all_devices is true. Optional field devices : list of devices. devices should be present and non empty when include_all_devices is either not present or false. Value should be present when device_group is empty. . Optional Field
id	-	String	Existing Raw Syslog Forwarder id . Obtain the value of the required Raw Syslog Forwarder id using RawSyslogForwarder - List API. Mandatory Field
pattern	Pattern	String	Pattern of logs to be collected and forwarded. Optional Field
remote_syslog_collectors	Remote Target	[String]	ID of the Targets where the logs are to be forwarded. Mandatory Field

Request Example

```
{
   "data": {
      "device_config": [
         {
            "device_group": "60a4a72c2d76c9046d54a3b6",
            "include_all_devices": true
         },
         {
```

(continues on next page)

(continued from previous page)

```
        "device_group": "40a4a72d2d76c9045d54a3b5",
        "devices": [
          "2344a72d2d76c9045d54a3c6",
          "5674a72d2d76c9045d54a3d7"
        ]
      }
    ],
    "pattern": "[ 0-9 ]+",
    "remote_syslog_collectors": [
      "60a4a72c2d76c9046d54a3b6",
      "31a4a72c2e66c9046d54a3c2"
    ]
  }
}
```

Success Response

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

39.4 RawSyslogForwarder - EditTarget

Edits the target settings with the given id

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/RawSyslogForwarder/
↪Target/{id}
```

Parameter

Field	Label in UI	Type	Description
enable_udp	Protocol	String	Accepts either "on" or "off" values only. "on" implies UDP while "off" implies TCP being selected as protocol for sending syslogmessage. Mandatory Field
id	-	String	Existing Target id . Obtain the value of the required Target id using Target - ListTarget API. Mandatory Field

Continued on next page

Table 4 – continued from previous page

Field	Label in UI	Type	Description
ip	IP	String	Ip address or hostname of the target device. Mandatory Field
name	Name	String	Name of the target. Mandatory Field
port	Port	int	Port number for the input port of the target. Mandatory Field

Request Example

```
{
  "data": {
    "enable_udp": "on",
    "ip": "10.45.6.15",
    "name": "target_1",
    "port": 514
  }
}
```

Success Response

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

39.5 RawSyslogForwarder - Get

Fetches the Raw Syslog Forwarder with the given id.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/RawSyslogForwarder/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	The id of the Raw Syslog Forwarder to fetch.

Success Response

```
{
   "device_config": [
      {
         "device_group": "60a4a72c2d76c9046d54a3b6",
         "include_all_devices": true
      },
      {
         "device_group": "40a4a72d2d76c9045d54a3b5",
         "devices": [
            "2344a72d2d76c9045d54a3c6",
            "5674a72d2d76c9045d54a3d7"
         ]
      }
   ],
   "id": "5c32c078f419a4aa901be3dc",
   "pattern": "[ 0-9 ]+",
   "remote_syslog_collectors": [
      "60a4a72c2d76c9046d54a3b6, 31a4a72c2e66c9046d54a3c2"
   ],
   "tid": ""
}
```

39.6 RawSyslogForwarder - GetTarget

Fetches the target with the given id

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/RawSyslogForwarder/
↪Target/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Id of the target whose information you want to fetch

Success Response

```
{
   "enable_udp": "on",
   "id": "5c32c078f419a4aa901be3dc",
   "ip": "10.45.3.91",
   "name": "target_1",
```

(continues on next page)

(continued from previous page)

```
    "port": "514",
    "tid": ""
}
```

39.7 RawSyslogForwarder - List

Lists all available Raw Syslog Forwarder.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/RawSyslogForwarder
```

Success Response

```
[
    {
        "device_config": [
            {
                "device_group": "60a4a72c2d76c9046d54a3b6",
                "include_all_devices": true
            },
            {
                "device_group": "40a4a72d2d76c9045d54a3b5",
                "devices": [
                    "2344a72d2d76c9045d54a3c6",
                    "5674a72d2d76c9045d54a3d7"
                ]
            }
        ],
        "id": "5c32c078f419a4aa901be3dc",
        "pattern": "[ 0-9 ]+",
        "remote_syslog_collectors": [
            "60a4a72c2d76c9046d54a3b6, 31a4a72c2e66c9046d54a3c2"
        ],
        "tid": ""
    }
]
```

39.8 RawSyslogForwarder - ListTarget

Lists all Targets in the Fabric-enabled Logpoint

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/RawSyslogForwarder/
↪Target
```

Success Response

```
[
  {
    "enable_udp": "on",
    "id": "5c32c078f419a4aa901be3dc",
    "ip": "10.45.3.91",
    "name": "target_1",
    "port": "514",
    "tid": ""
  }
]
```

39.9 RawSyslogForwarder - Trash

Delete the Raw Syslog Forwarder with given id.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/RawSyslogForwarder/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing Raw Syslog Forwarder id . Obtain the value of the required Raw Syslog Forwarder id using RawSyslogForwarder - List API. Mandatory Field

Success Response

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

39.10 RawSyslogForwarder - TrashTarget

Deletes the Target with the given id

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/RawSyslogForwarder/
↪Target/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing Target id . Obtain the value of the required Target id using Target - ListTarget API. Mandatory Field

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

FORTY

REFRESHTOKEN

40.1 RefreshToken - Create

Generates new token and secretkey for public facing API. For more details, refer to Director Console Manual v1.4.0. or above.

POST

```
https://api-server-host-name/refreshToken
```

Parameter

Field	Label in UI	Type	Description
secretKey	-	String	Secret key of old token. Mandatory Field

Request Example

```
{
  "secretKey": "861979e1-4071-4dff-9725-b900c43502d3"
}
```

Success Response

```
{
  "status": "Success",
  "tokenDetails": {
    "secretKey": "861979e1-4071-4dff-9725-b900c43502d3",
    "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
↪eyJ1c2VyIjp7InN1Y2Nlc3MiOjEsIl9rZXkiOiI1MjEyNDQ0IiwiX2lkIjoidXNlcnMvNTIxMjQ0NCIsInVzZXJuYW1lIjoiZ
↪Zk05wiJuBpeEnMYEwPS9OEmHzwPANE1m3z1R3AFkPtw"
  }
}
```

CHAPTER

FORTYONE

REPOS

41.1 Repos - Create

Creates a new Repo.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Repos
```

Parameter

Field	Label in UI	Type	Description
hiddenrepopath	Repo Path, Retention (day)	[json]	Consists information about path (string) assigned for the Repo and the retention (int) time for the data. Use Repos - ListRepoPaths API to obtain the value of the required Repo Path. Mandatory Field
name	Repo Name	String	Repo name . Mandatory Field
repoha	Remote LogPoint, Available for (day)	[json]	Lists the information for remote LogPoints. It contains following parameters: ha_li: remote LogPoint private IP (string) ha_day: retention days (int). Optional Field

Request Example

```
{
   "data": {
      "hiddenrepopath": [
         {
            "path": "/opt/immune/storage/",
```

(continues on next page)

(continued from previous page)

```
                "retention": 36
            }
        ],
        "name": "test1",
        "repoha": [
            {
                "ha_day": 2,
                "ha_li": "10.218.261.2"
            }
        ]
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

41.2 Repos - Edit

Edits a Repo with given ID.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Repos/{id}
```

Parameter

Field	Label in UI	Type	Description
hiddenrepopath	Repo Path, Retention (day)	[json]	Consists information about path (string) assigned for the Repo and the retention (int) time for the data. Use Repos - ListRepoPaths API to obtain the value of the required Repo Path. Mandatory Field
id	-	String	Existing repo_id . Mandatory Field

Continued on next page

Table 2 – continued from previous page

Field	Label in UI	Type	Description
repoha	Remote LogPoint, Available for (day)	[json]	Lists the information for remote LogPoints. It contains following parameters: ha_li: remote LogPoint private IP (string) ha_day: retention days (int). Optional Field

Request Example

```
{
  "data": {
    "hiddenrepopath": [
      {
        "path": "/opt/immune/storage/",
        "retention": 36
      }
    ],
    "repoha": [
      {
        "ha_day": 5,
        "ha_li": "10.218.261.2"
      }
    ]
  }
}
```

Success Response

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

41.3 Repos - FetchRemoteRepos

Fetches all local and remote Repos.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Repos/RemoteRepos/
↪fetch
```

Request Example

```
{
   "data": {}
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}/{data_node}"
}
```

41.4 Repos - Get

Fetches the Repo with given ID.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Repos/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing Repo id .

Success Response

```
{
   "active": true,
   "id": "5a466fc9d8aaa4748d3977c9",
   "name": "default",
   "repo_number": 1,
   "repoha": [],
   "repopath": [
      {
         "path": "/opt/immune/storage/",
         "retention": 365
      }
   ],
   "tid": "",
   "used_size": "1.24268 MB"
}
```

41.5 Repos - List

Lists all available Repos.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Repos
```

Success Response

```
[
    {
        "active": true,
        "id": "5a466fc9d8aaa4748d3977c9",
        "name": "default",
        "repo_number": 1,
        "repoha": [],
        "repopath": [
            {
                "path": "/opt/immune/storage/",
                "retention": 365
            }
        ],
        "tid": "",
        "used_size": "1.24268 MB"
    }
]
```

41.6 Repos - ListRepoPaths

Lists all allowed Repo Paths.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Repos/RepoPaths
```

Success Response

```
[
    {
        "paths": [
            "/opt/immune/storage/"
        ]
    }
]
```

41.7 Repos - RefreshRepoPaths

Syncs LogPoint's Repo Path List to the current Repo Path list.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Repos/RepoPaths/
↪refreshlist
```

Request Example

```
{
   "data": {}
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

41.8 Repos - Trash

Deletes a Repo with given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Repos/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing Repo id . Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

FORTYTWO

ROUTINGPOLICIES

42.1 RoutingPolicies - Create

Creates a new Routing Policy.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/RoutingPolicies
```

Parameter

Field	Label in UI	Type	Description
catch_all	Catch All	String	It is the default Repo. If none of the routing criteria matches then the default repo is selected. Mandatory Field
policy_name	Policy Name	String	Routing Policy name. Mandatory Field

Continued on next page

Table 1 – continued from previous page

Field	Label in UI	Type	Description
routing_criteria	Routing Criteria	[json]	This field can be an empty List [ ] if Routing criteria doesn't need to be defined. To define **routing criteria**, you must provide the following parameters: • *category*: Value can be "simple" or "type_based". • *operation*: Value must be "Equals". • *prefix*: Value can be "true" or "false". Mandatory only when category = "type_based". • *event_key*: Event id. Mandatory only when category = "simple". • *source_key*: Source id. • *type*: Value can only be "ip" or "string" or "num". Mandatory only when category = "type_based".

Request Example

```
{
  "data": {
    "catch_all": "default",
    "routing_criteria": [
      {
        "repo": "_logpoint",
```

(continues on next page)

(continued from previous page)

```
                "drop": "store",
                "type": "KeyPresent",
                "key": "aa",
                "value": ""
            },
            {
                "repo": "",
                "drop": "store",
                "type": "KeyPresentValueMatches",
                "key": "hh",
                "value": "oo"
            }
        ],
        "policy_name": "testPolicy"
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

42.2 RoutingPolicies - Edit

Edits the Routing Policy with given ID.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/RoutingPolicies/{id}
```

Parameter

Field	Label in UI	Type	Description
policy_name	Policy Name	String	Routing Policy name . Mandatory Field
catch_all	Catch All	String	It is the default repo. If none of the routing criteria is matched then the default repo is selected. Mandatory Field
id	-	String	Routing Policy id . Mandatory Field

Continued on next page

Table 2 – continued from previous page

Field	Label in UI	Type	Description
routing_criteria	Routing Criteria	[json]	This field can be an empty List [ ] if Routing criteria doesn't need to be defined. To define **routing criteria**, you must provide the following parameters: • *category*: Value can be "simple" or "type_based". • *operation*: Value must be "Equals". • *prefix*: Value can be "true" or "false". Mandatory only when category = "type_based". • *event_key*: Event id. Mandatory only when category = "simple". • *source_key*: Source id. • *type*: Value can only be "ip" or "string" or "num". Mandatory only when category = "type_based".

Request Example

```
{
   "data": {
      "routing_criteria": [
         {
            "repo": "_logpoint",
            "drop": "store",
```

(continues on next page)

(continued from previous page)

```
                "type": "KeyPresent",
                "key": "aa",
                "value": ""
            },
            {
                "repo": "",
                "drop": "store",
                "type": "KeyPresentValueMatches",
                "key": "hh",
                "value": "oo"
            }
        ],
        "policy_name": "testPolicy",
        "catch_all": "default"
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

42.3 RoutingPolicies - Get

Fetches a Routing Policy with given ID.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/RoutingPolicies/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Routing Policy id .

Success Response

```
{
    "routing_criteria": [
        {
            "type": "KeyPresent",
            "key": "aa",
```

(continues on next page)

(continued from previous page)

```
            "value": "",
            "repo": "_logpoint",
            "drop": "store"
        },
        {
            "type": "KeyPresentValueMatches",
            "key": "hh",
            "value": "oo",
            "repo": "",
            "drop": "store"
        }
    ],
    "policy_name": "testPolicy",
    "catch_all": "default",
    "id": "574fb123d8aaa4625bfe2d23"
}
```

42.4 RoutingPolicies - List

Lists all Routing Policies.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/RoutingPolicies
```

Success Response

```
[
    {
        "catch_all": "default",
        "routing_criteria": [
            {
                "repo": "_logpoint",
                "drop": "store",
                "type": "KeyPresent",
                "key": "aa",
                "value": ""
            },
            {
                "repo": "",
                "drop": "store",
                "type": "KeyPresentValueMatches",
                "key": "hh",
                "value": "oo"
```

(continues on next page)

(continued from previous page)

```
            }
        ],
        "policy_name": "testPolicy",
        "id": "574fb123d8aaa4625bfe2d23"
    }
]
```

42.5 RoutingPolicies - Trash

Deletes the Routing Policy with given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/RoutingPolicies/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Routing Policy id . Mandatory Field

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

FORTYTHREE

SEARCH

43.1 Search - FetchSearchLogs

Fetch all search logs based on given conditions

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Search/logs/fetch
```

Parameter

Field	Label in UI	Type	Description
limit		int	The maximum number of rows returned in a single request. The default value of the limit parameter is 100. Optional Field
query		String	Valid LogPoint query to filter the response based on the given query. Mandatory Field
repos		[String]	List of repos where the logs are searched. Fetch the list of available repos using the Repos - FetchRemoteRepos API. The endpoint returns logs from all the permitted repos if the repos parameter is absent in the request. Optional Field
time_range		[String]	Starting and ending Unix time stamp to define the time range for the logs. The endpoint returns the logs that were recorded between the given time range. Mandatory Field

Continued on next page

Table 1 – continued from previous page

Field	Label in UI	Type	Description
user_id		String	Existing User id. Fetch the list of users with the Users - List API. Mandatory Field

Request Example

```
{
   "data": {
      "limit": 100,
      "query": "| chart count() by device_ip",
      "repos": [
         "127.0.0.1:5504/_logpoint",
         "10.4.0.1:5504/_logpoint"
      ],
      "time_range": [
         "880968071",
         "1637832071"
      ],
      "user_id": "5d88c559d8aaa42d8c4bfc41"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}/{data_node}"
}
```

CHAPTER

FORTYFOUR

SEARCHLABELS

44.1 SearchLabels - Activate

Activates the search label with given id .

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SearchLabels/{id}/
↪activate
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing search label ID. Mandatory Field

Request Example

```
{
   "data": {}
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

44.2 SearchLabels - Create

Creates a new search label in a Fabric-enabled LogPoint.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SearchLabels
```

Parameter

Field	Label in UI	Type	Description
package_id	Package	String	ID of the label package. Obtain the value of the required Label Package id using LabelPackages - List API. Mandatory Field
search_label	List of Labels	[String]	List of the labels. Mandatory Field
search_query	Search Query	String	Complete and valid Query or value can contain the name of the existing Macros inside ”. Optional Field

Request Example

```
{
   "data": {
      "package_id": "574fceedd8aaa40740736302",
      "search_label": [
         "ip",
         "device_ip"
      ],
      "search_query": "device_ip=127.0.0.1"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

44.3 SearchLabels - Deactivate

Deactivates the search label with given id .

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SearchLabels/{id}/
↪deactivate
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing search label ID. Mandatory Field

Request Example

```
{
   "data": {}
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

44.4 SearchLabels - Edit

Edits the search label with given ID in a Fabric-enabled LogPoint.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SearchLabels/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing Search Label id . Obtain the value of the required Search Label id using SearchLabels - List API. Mandatory Field
search_label	List of Labels	[String]	List of the labels. Mandatory Field
search_query	Search Query	String	Complete and valid Query or value can contain the name of the existing Macros inside ". Optional Field

Request Example

```
{
   "data": {
      "search_label": [
         "ip",
         "device_ip"
      ],
      "search_query": "device_ip=127.0.0.1"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

44.5 SearchLabels - Trash

Removes the search label with given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SearchLabels/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	ID of the existing search label that you want to delete. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

FORTYFIVE

SCPFETCHER

45.1 SCPFetcher - Create

Create SCP fetcher with device ID

POST

https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SCPFetcher

Parameter

Field	Label in UI	Type	Description
auth_type	Authentication	String	password or certificate (exact). Mandatory Field
username	Username	String	SCP username. Mandatory Field
parser	Parser	String	Value can be one of the following: SyslogParser LineParser StackTraceParser DB2Parser RACFParser or any custom parser. Mandatory Field
interval	Fetch Interval (minutes)	int	Fetch interval in minutes. Mandatory Field
processpolicy	Processing Policy	String	Select a Processing Policy for the collector. Execute ProcessingPolicy - List API to list the available processpolicies and use the value of the id parameter. Mandatory Field
namepattern	Filename Pattern	String	Regex pattern for filename match or empty for all. Optional Field
port	Port	int	Access port. Mandatory Field

Continued on next page

Table 1 – continued from previous page

Field	Label in UI	Type	Description
oldlogs	Forward Old Logs	String	Check point to extract old logs or not - If check should be "on" or "off" (exact). Mandatory Field
device_id	-	String	Existing Device id . Obtain the value of the required device_id using Devices - List API. Optional Field
auth_password	Password	String	Password for authentication. Only mandatory if auth_type is equal to 'password'. Mandatory Field
charset	Charset	String	Existing LogPoint charset. Obtain the value of the required charset using Charsets - List API. Mandatory Field
remotepath	Relative FilePath	String	Remote path to the file directory. Optional Field.
policy_id	-	String	Respective LCP policy ID. Obtain the value of the required policy_id using LogCollectionPolicies - List API. Optional Field

Request Example

```
{
   "data": {
      "auth_type": "password",
      "username": "SCPTest",
      "parser": "SyslogParser",
      "interval": 6,
      "processpolicy": "57724aacd8aaa40b569bcb1fasd",
      "namepattern": "*.pyc",
      "port": 22,
      "oldlogs": "on",
      "device_id": "57724aacd8aaa40b569bcb1f",
      "auth_password": "hercules",
      "charset": "utf_8",
      "remotepath": "/base/collection/"
   }
}
```

Success Response

```
{
```

(continues on next page)

(continued from previous page)

```
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

45.2 SCPFetcher - Edit

Edit SCP with given ID

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SCPFetcher/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	UUID of the respective SCPFetcher. To obtain the SCP fetcher uuid , execute Devices - List API if the collector was configured using device id or execute LogCollectionPolicies - List API if the collector was configured using log collection policy id . Mandatory Field
processpolicy	Processing Policy	String	Pick one from the available process policy id from the database. Mandatory Field
charset	Charset	String	Existing LogPoint charset. Obtain the value of the required charset using Charsets - List API. Mandatory Field
auth_type	Authentication	String	password or certificate (exact). Mandatory Field
username	Username	String	SCP username. Mandatory Field
remotepath	Relative FilePath	String	Remote path to the file directory. Optional Field
namepattern	Filename Pattern	String	Regex pattern for filename match or empty for all. Optional Field
port	Port	int	Access port. Mandatory Field

Continued on next page

Table 2 – continued from previous page

Field	Label in UI	Type	Description
parser	Parser	String	Value can be one of the following: SyslogParser LineParser StackTraceParser DB2Parser RACFParser . Mandatory Field
interval	Fetch Interval (minutes)	int	Fetch interval in minutes. Mandatory Field
oldlogs	Forward Old Logs	String	Check point to extract old logs or not - If check should be "on" or "off" (exact). Mandatory Field
auth_password	Password	String	Password for authentication. Only mandatory if auth_type is equal to 'password'. Mandatory Field

Request Example

```
{
   "data": {
      "processpolicy": "57724aacd8aaa40b569bcb1fasd",
      "charset": "utf_8",
      "auth_type": "password",
      "username": "SCPTest",
      "remotepath": "/base/collection/",
      "namepattern": "*.pyc",
      "port": 22,
      "parser": "SyslogParser",
      "interval": 6,
      "oldlogs": "on",
      "auth_password": "hercules"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

45.3 SCPFetcher - TestExisting

Test existing SCP connection

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SCPFetcher/{id}/
↪testexistingscp
```

Parameter

Field	Label in UI	Type	Description
id	-	String	UUID of the respective SCPFetcher. Obtain the value of the required SCPFetcher uuid using Devices - List API. Mandatory Field

Request Example

```
{
   "data": {}
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

45.4 SCPFetcher - TestNew

Test new SCP fetcher with device ID

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SCPFetcher/
↪testnewscp
```

Parameter

Field	Label in UI	Type	Description
auth_type	Authentication	String	password or certificate (exact). Mandatory Field
username	Username	String	SCP username. Mandatory Field

Continued on next page

Table 4 – continued from previous page

Field	Label in UI	Type	Description
parser	Parser	String	Value can be one of the following: SyslogParser LineParser StackTraceParser DB2Parser RACFParser or any custom parser. Mandatory Field
device_id	-	String	Existing Device id . Obtain the value of the required device_id using Devices - List API. Optional Field
interval	Fetch Interval (minutes)	int	Fetch interval in minutes. Mandatory Field
processpolicy	Processing Policy	String	Select a Processing Policy for the collector. Execute ProcessingPolicy - List API to list the available processpolicies and use the value of the id parameter. . Mandatory Field
namepattern	Filename Pattern	String	Regex pattern for filename match or empty for all. Optional Field
port	Port	int	Access port. Mandatory Field
oldlogs	Forward Old Logs	String	Check point to extract old logs or not - If check should be "on" or "off" (exact). Mandatory Field
auth_password	Password	String	Password for authentication. Only mandatory if auth_type is equal to 'password'. Mandatory Field
charset	Charset	String	Existing LogPoint charset. Obtain the value of the required charset using Charsets - List API. Mandatory Field
remotepath	Relative FilePath	String	Remote path to the file directory. Optional Field

Request Example

```
{
  "data": {
    "auth_type": "password",
    "username": "SCPTest",
    "parser": "SyslogParser",
    "device_id": "57724aacd8aaa40b569bcb1f",
```

(continues on next page)

(continued from previous page)

```
        "interval": 6,
        "processpolicy": "57724aacd8aaa40b569bcb1fasd",
        "namepattern": "*.pyc",
        "port": 22,
        "oldlogs": "on",
        "auth_password": "hercules",
        "charset": "utf_8",
        "remotepath": "/base/collection/"
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

45.5 SCPFetcher - Trash

Delete the SCP fetcher with given ID

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SCPFetcher/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	UUID of the respective SCPFetcher. To obtain the SCP fetcher uuid , execute Devices - List API if the collector was configured using device id or execute LogCollectionPolicies - List API if the collector was configured using log collection policy id . Mandatory Field

Success Response

```
{
    "status": "Success",
```

(continues on next page)

(continued from previous page)

```
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

FORTYSIX

SFLOWCOLLECTORPLUGIN

46.1 SFlowCollectorPlugin - Create

Creates a new SFlow Collector Plugin.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SFlowCollectorPlugin
```

Parameter

Field	Label in UI	Type	Description
device_id	-	String	Device id . Use the value of the id parameter of the required Devices from the Devices - List API. Optional Field
policy_id	-	String	Respective LCP policy ID. Obtain the value of the required policy_id using LogCollectionPolicies - List API. Optional Field
processpolicy	Processing Policy	String	Existing Processing Policy id or None (exact). Use the value of the id parameter from ProcessingPolicy - List API to obtain Processing Policy id . Mandatory Field

Request Example

```
{
   "data": {
      "device_id": "57724aacd8aaa40b569bcb1f",
      "processpolicy": "57724aacd8aaa40b569bcb1fasd"
   }
```

(continues on next page)

(continued from previous page)

```
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

46.2 SFlowCollectorPlugin - Edit

Edits an SFlow Collector Plugin with given ID.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SFlowCollectorPlugin/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	SFlow Collector uuid . To obtain the SFlow Collector uuid , execute Devices - List API if the collector was configured using device id or execute LogCollectionPolicies - List API if the collector was configured using log collection policy id . Mandatory Field
processpolicy	Processing Policy	String	Existing Processing Policy id or None (exact). Use the value of the id parameter from ProcessingPolicy - List API to obtain Processing Policy id . Mandatory Field

Request Example

```
{
   "data": {
      "processpolicy": "57724aacd8aaa40b569bcb1fasd"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

46.3 SFlowCollectorPlugin - Trash

Deletes an SFlow Collector Plugin with given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SFlowCollectorPlugin/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	SFlow Collector uuid . To obtain the SFlow Collector uuid , execute Devices - List API if the collector was configured using device id or execute LogCollectionPolicies - List API if the collector was configured using log collection policy id . Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

FORTYSEVEN

SNARECOLLECTORPLUGIN

47.1 SnareCollectorPlugin - Create

Creates a Snare Collector Plugin using device ID or policy ID.

POST

https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SnareCollectorPlugin

Parameter

Field	Label in UI	Type	Description
charset	Charset	String	Existing LogPoint charset. Obtain the value of the required charset using Charsets - List API. Mandatory Field
device_id	-	String	Device id . Use the value of the id parameter of the required Devices from the Devices - List API. Optional Field
parser	Parser	String	Existing Parser name or None (exact). Use the value of the name parameter from Parsers - List API. Mandatory Field
policy_id	-	String	Respective LCP policy ID. Obtain the value of the required policy_id using LogCollectionPolicies - List API. Optional Field

Continued on next page

Table 1 – continued from previous page

Field	Label in UI	Type	Description
processpolicy	Processing Policy	String	Existing Processing Policy id or None (exact). Use the value of the id parameter of the required Processing Policy from ProcessingPolicy - List API. Mandatory Field

Request Example

```
{
  "data": {
    "charset": "utf_8",
    "device_id": "57724aacd8aaa40b569bcb1f",
    "parser": "LineParser",
    "processpolicy": "57724aacd8aaa40b569bcb1fasd"
  }
}
```

Success Response

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

47.2 SnareCollectorPlugin - Edit

Edits the Snare Collector Plugin with given ID.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SnareCollectorPlugin/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
charset	Charset	String	Existing LogPoint charset. Obtain the value of the required charset using Charsets - List API. Mandatory Field

Continued on next page

Table 2 – continued from previous page

Field	Label in UI	Type	Description
id	-	String	Existing Snare Collector Plugin uuid . To obtain the Snare collector uuid , execute Devices - List API if the collector was configured using device id or execute LogCollectionPolicies - List API if the collector was configured using log collection policy id . Mandatory Field
parser	Parser	String	Existing Parser name or None (exact). Use the value of the name parameter from Parsers - List API. Mandatory Field
processpolicy	Processing Policy	String	Existing Processing Policy id or None (exact). Use the value of the id parameter of the required Processing Policy from ProcessingPolicy - List API. Mandatory Field

Request Example

```
{
   "data": {
      "charset": "utf_8",
      "parser": "LineParser",
      "processpolicy": "57724aacd8aaa40b569bcb1fasd"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

47.3 SnareCollectorPlugin - Trash

Deletes the Snare Collector Plugin with given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SnareCollectorPlugin/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing Snare Collector Plugin uuid . To obtain the Snare collector uuid , execute Devices - List API if the collector was configured using device id or execute LogCollectionPolicies - List API if the collector was configured using log collection policy id . Mandatory Field

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

FORTYEIGHT

SNMPFETCHER

48.1 SNMPFetcher - Create

Creates an SNMP fetcher with device ID.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SNMPFetcher
```

Parameter

Field	Label in UI	Type	Description
authkey	Authorization Key	String	Authentication key. Mandatory only when the value of the snmpver parameter is "v_3". Optional Field
charset	Charset	String	Existing LogPoint charset. Obtain the value of the required charset using Charsets - List API. Mandatory Field
communitystring	Community String	String	Authentication string. Mandatory only when the value of the snmpver parameter is "v_12". Optional Field
device_id	-	String	Device id . Use the value of the id parameter of the required Devices from the Devices - List API. Optional Field
policy_id	-	String	Respective LCP policy ID. Obtain the value of the required policy_id using LogCollectionPolicies - List API. Optional Field

Continued on next page

Table 1 – continued from previous page

Field	Label in UI	Type	Description
port	Port	int	Access Port number. Mandatory Field
privkey	Private Key	String	Encryption key. Mandatory only when the value of the snmpver parameter is "v_3". Optional Field
processpolicy	Processing Policy	String	Existing Processing Policy id or None (exact). Use the value of the id parameter from ProcessingPolicy - List API to obtain Processing Policy id . Mandatory Field
snmp_policy	SNMP Policy	String	SNMP Policy name . Use the value of name parameter of the required SNMP Policy from the SNMPPolicy - List API. Mandatory Field
snmpver	SNMP Version	String	Value must be "v_3" or "v_12". Mandatory Field
username	Username	String	SNMP username . Mandatory only when the value of the snmpver parameter is "v_3". Optional Field

Request Example

```
{
   "data": {
      "authkey": "adjfghnljen12412452",
      "charset": "utf_8",
      "device_id": "57724aacd8aaa40b569bcb1f",
      "port": 161,
      "privkey": "adsfjadls;jfhgaosdh1235423523",
      "processpolicy": "57724aacd8aaa40b569bcb1fasd",
      "snmp_policy": "windows_snmp",
      "snmpver": "v_3",
      "username": "SNMPTest"
   }
}
```

Success Response

```
{
```

(continues on next page)

(continued from previous page)

```
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

48.2 SNMPFetcher - Edit

Edits an SNMP fetcher with given ID.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SNMPFetcher/{id}
```

Parameter

Field	Label in UI	Type	Description
authkey	Authorization Key	String	Authentication key. Mandatory only when the value of the snmpver parameter is "v_3". Optional Field
charset	Charset	String	Existing LogPoint charset. Obtain the value of the required charset using Charsets - List API. Mandatory Field
communitystring	Community String	String	Authentication string. Mandatory only when the value of the snmpver parameter is "v_12". Optional Field
id	-	String	SNMP Fetcher uuid . To obtain the SNMP fetcher uuid , execute Devices - List API if the collector was configured using device id or execute LogCollectionPolicies - List API if the collector was configured using log collection policy id . Mandatory Field
port	Port	int	Access Port number. Mandatory Field
privkey	Private Key	String	Encryption key. Mandatory only when the value of the snmpver parameter is "v_3". Optional Field

Continued on next page

Table 2 – continued from previous page

Field	Label in UI	Type	Description
processpolicy	Processing Policy	String	Existing Processing Policy id or None (exact). Use the value of the id parameter from ProcessingPolicy - List API to obtain Processing Policy id . Mandatory Field
snmp_policy	SNMP Policy	String	SNMP Policy name . Use the value of name parameter of the required SNMP Policy from the SNMPPolicy - List API. Mandatory Field
snmpver	SNMP Version	String	Value must be "v_3" or "v_12". Mandatory Field
username	Username	String	SNMP username . Mandatory only when the value of the snmpver parameter is "v_3". Optional Field

Request Example

```
{
   "data": {
      "authkey": "adjfghnljen12412452",
      "charset": "utf_8",
      "port": 161,
      "privkey": "adsfjadls;jfhgaosdh1235423523",
      "processpolicy": "57724aacd8aaa40b569bcb1fasd",
      "snmp_policy": "windows_snmp",
      "snmpver": "v_3",
      "username": "SNMPTest"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

48.3 SNMPFetcher - TestExisting

Tests the existing SNMP Fetcher connection.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SNMPFetcher/{id}/
↪testexistingsnmp
```

Parameter

Field	Label in UI	Type	Description
id	-	String	SNMPFetcher uuid . Use the id of the required SNMP Fetcher from the Devices - List API. Mandatory Field

Request Example

```
{
    "data": {}
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

48.4 SNMPFetcher - TestNew

Tests the newly created SNMP Fetcher connection.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SNMPFetcher/
↪testnewsnmp
```

Parameter

Field	Label in UI	Type	Description
authkey	Authorization Key	String	Authentication key. Mandatory only when the value of the snmpver parameter is "v_3". Optional Field

Continued on next page

Table 4 – continued from previous page

Field	Label in UI	Type	Description
charset	Charset	String	Existing LogPoint charset. Obtain the value of the required charset using Charsets - List API. Mandatory Field
communitystring	Community String	String	Authentication string. Mandatory only when the value of the snmpver parameter is "v_12". Optional Field
device_id	-	String	Device id . Use the value of the id parameter of the required Devices from the Devices - List API. Mandatory Field
port	Port	int	Access Port number. Mandatory Field
privkey	Private Key	String	Encryption key. Mandatory only when the value of the snmpver parameter is "v_3". Optional Field
processpolicy	Processing Policy	String	Existing Processing Policy id or None (exact). Use the value of the id parameter from ProcessingPolicy - List API to obtain Processing Policy id . Mandatory Field
snmp_policy	SNMP Policy	String	SNMP Policy name . Use the value of name parameter of the required SNMP Policy from the SNMPPolicy - List API. Mandatory Field
snmpver	SNMP Version	String	Value must be "v_3" or "v_12". Mandatory Field
username	Username	String	SNMP username . Mandatory only when the value of the snmpver parameter is "v_3". Optional Field

Request Example

```
{
   "data": {
      "authkey": "adjfghnljen12412452",
      "charset": "utf_8",
```

(continues on next page)

(continued from previous page)

```
        "device_id": "57724aacd8aaa40b569bcb1f",
        "port": 161,
        "privkey": "adsfjadls;jfhgaosdh1235423523",
        "processpolicy": "57724aacd8aaa40b569bcb1fasd",
        "snmp_policy": "windows_snmp",
        "snmpver": "v_3",
        "username": "SNMPTest"
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

48.5 SNMPFetcher - Trash

Deletes the SNMP Fetcher with given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SNMPFetcher/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	SNMP Fetcher uuid . To obtain the SNMP fetcher uuid , execute Devices - List API if the collector was configured using device id or execute LogCollectionPolicies - List API if the collector was configured using log collection policy id . Mandatory Field

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

FORTYNINE

SNMPPOLICY

49.1 SNMPPolicy - Create

Creates a new SNMP Policy.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SNMPPolicy
```

Parameter

Field	Label in UI	Type	Description
name	Name	String	SNMP Policy name. Mandatory Field
oid_time	Policy	[json]	SNMP oid key and fetch time in minutes. Mandatory Field

Request Example

```
{
   "data": {
      "name": "testPolicy",
      "oid_time": [
         {
            "field": "1.3.6.1.2.1.1.5.0",
            "value": 5
         },
         {
            "field": "1.3.6.1.3.2.1.5.0",
            "value": 6
         }
      ]
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

49.2 SNMPPolicy - Edit

Edits the SNMP Policy with given ID.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SNMPPolicy/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing SNMP Fetcher id . Mandatory Field
name	Name	String	name of the snmp policy. Mandatory Field
oid_time	Policy	[json]	SNMP oid key and fetch time in minutes. Mandatory Field

Request Example

```
{
   "data": {
      "name": "testPolicy",
      "oid_time": [
         {
            "field": "1.3.6.1.2.1.1.5.0",
            "value": 5
         },
         {
            "field": "1.3.6.1.3.2.1.5.0",
            "value": 6
         }
      ]
   }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

49.3 SNMPPolicy - Get

Fetches an SNMP Policy with given ID.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SNMPPolicy/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing SNMP Policy id .

Success Response

```
{
    "id": "574fb123d8aaa4625bfe2d23",
    "name": "testPolicy",
    "oid_time": [
        {
            "field": "1.3.6.1.2.1.1.5.0",
            "value": 5
        },
        {
            "field": "1.3.6.1.3.2.1.5.0",
            "value": 6
        }
    ]
}
```

49.4 SNMPPolicy - List

Lists all SNMP Policies.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SNMPPolicy
```

Success Response

```
[
  {
    "id": "574fb123d8aaa4625bfe2d23",
    "name": "testPolicy",
    "oid_time": [
      {
        "field": "1.3.6.1.2.1.1.5.0",
        "value": 5
      },
      {
        "field": "1.3.6.1.3.2.1.5.0",
        "value": 6
      }
    ]
  }
]
```

49.5 SNMPPolicy - Trash

Deletes the SNMP Policy with given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SNMPPolicy/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing SNMP Policy id . Mandatory Field

Success Response

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

FIFTY

SNMPTRAPCOLLECTOR

50.1 SNMPTrapCollector - Create

Creates an SNMP Trap Collector.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SNMPTrapCollector
```

Parameter

Field	Label in UI	Type	Description
authkey	Authorization Key	String	Authentication key. Mandatory only when the value of the snmpver parameter is "v_3". Optional Field
communitystring	Community String	String	Authentication string. Mandatory only when the value of the snmpver parameter is "v_12". Optional Field
device_id	-	String	Existing Device id . Obtain the value of the required device_id using Devices - List API. Optional Field
engineId	Security Engine ID	String	Identifier of the remote SNMP protocol engine. Mandatory only when the value of the snmpver parameter is "v_3". Optional Field
policy_id	-	String	Respective LCP policy ID. Obtain the value of the required policy_id using LogCollectionPolicies - List API. Optional Field

Continued on next page

Table 1 – continued from previous page

Field	Label in UI	Type	Description
privkey	Private Key	String	Encryption key. Mandatory only when the value of the snmpver parameter is "v_3". Optional Field
processpolicy	Processing Policy	String	Existing Processing Policy id or None (exact). Use the value of the id parameter of the required Processing Policy from ProcessingPolicy - List API. Mandatory Field
snmpver	SNMP Version	String	Value must be "v_3" or "v_12". Mandatory Field
username	Username	String	SNMP username. Mandatory only when the value of the snmpver parameter is "v_3". Optional Field

Request Example

```
{
   "data": {
      "communitystring": "public",
      "device_id": "57724aacd8aaa40b569bcb1f",
      "processpolicy": "57724aacd8aaa40b569bcb1fasd",
      "snmpver": "v_12"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

50.2 SNMPTrapCollector - Edit

Edits the SNMP Trap Collector with given ID.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SNMPTrapCollector/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
authkey	Authorization Key	String	Authentication key.Mandatory only when the value of the snmpver parameter is "v_3". Optional Field
communitystring	Community String	String	Authentication string. Mandatory only when the value of the snmpver parameter is "v_12". Optional Field
engineId	Security Engine ID	String	Identifier of the remote SNMP protocol engine. Mandatory only when the value of the snmpver parameter is "v_3". Optional Field
id	-	String	SNMP Trap Collector uuid . To obtain the SNMP trap collector uuid , execute Devices - List API if the collector was configured using device id or execute LogCollectionPolicies - List API if the collector was configured using log collection policy id . Mandatory Field
privkey	Private Key	String	Encryption key. Mandatory only when the value of the snmpver parameter is "v_3". Optional Field
processpolicy	Processing Policy	String	Existing Processing Policy id or None (exact). Use the value of the id parameter of the required Processing Policy from ProcessingPolicy - List API. Mandatory Field
snmpver	SNMP Version	String	Value must be "v_3" or "v_12". Mandatory Field
username	Username	String	SNMP username. Mandatory only when the value of the snmpver parameter is "v_3". Optional Field

Request Example

```
{
  "data": {
    "communitystring": "public",
    "processpolicy": "57724aacd8aaa40b569bcb1fasd",
    "snmpver": "v_12"
  }
}
```

Success Response

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

50.3 SNMPTrapCollector - Trash

Deletes the SNMP Trap Collector with given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SNMPTrapCollector/
↪{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	SNMP Trap Collector uuid . To obtain the SNMP trap collector uuid , execute Devices - List API if the collector was configured using device id or execute LogCollectionPolicies - List API if the collector was configured using log collection policy id . Mandatory Field

Success Response

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

FIFTYONE

SYSLOGCOLLECTOR

51.1 SyslogCollector - Create

Creates a Syslog Collector.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SyslogCollector
```

Parameter

Field	Label in UI	Type	Description
charset	Charset	String	Existing LogPoint charset. Obtain the value of the required charset using Charsets - List API. Mandatory only when proxy_condition is use_as_proxy or None. Optional Field
device_id	-	String	Existing Device id . Obtain the value of the required device_id using Devices - List API. Optional Field
hostname	HostName	[String]	List of server hostname of the Server(s) where the value of the proxy_condition parameter is "uses_proxy". Optional Field

Continued on next page

Table 1 – continued from previous page

Field	Label in UI	Type	Description
parser	Parser	String	Value must be one of the following: SyslogParser LineParser MultiLineSyslogParser ProofPointEmailProtectionLogParser EmailParser Mandatory only when the value of the proxy_condition parameter is "use_as_proxy" or "None". Optional Field
policy_id	-	String	Respective LCP policy ID. Obtain the value of the required policy_id using LogCollectionPolicies - List API. Optional Field
processpolicy	Processing Policy	String	Existing Processing Policy id or "None". Execute the ProcessingPolicy - List API to obtain the value of the required Processing Policy id . Mandatory only when the value of 'proxy_condition' is "uses_proxy" or "None". Optional Field
proxy_condition	Proxy Server	String	Value can be "uses_proxy", "use_as_proxy" or "None". Mandatory Field
proxy_ip	Proxy IP	[String]	List of IP address of the Proxy Server(s) where the value of the proxy_condition parameter is "uses_proxy". Optional Field

Request Example

```
{
   "data": {
      "device_id": "57724aacd8aaa40b569bcb1f",
      "hostname": [
         "Logpoint"
      ],
      "processpolicy": "57724aacd8aaa40b569bcb1fasd",
      "proxy_condition": "uses_proxy",
      "proxy_ip": [
         "1.1.1.1"
      ]
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

51.2 SyslogCollector - Edit

Edits the Syslog Collector with given ID.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SyslogCollector/{id}
```

Parameter

Field	Label in UI	Type	Description
charset	Charset	String	Existing LogPoint charset. Obtain the value of the required charset using Charsets - List API. Mandatory only when proxy_condition is use_as_proxy or None. Optional Field
hostname	HostName	[String]	List of server hostname of the Server(s) where the value of the proxy_condition parameter is "uses_proxy". Optional Field
id	-	String	UUID of the respective SyslogCollector. To obtain the Syslog collector uuid , execute Devices - List API if the collector was configured using device id or execute LogCollectionPolicies - List API if the collector was configured using log collection policy id . Mandatory Field

Continued on next page

Table 2 – continued from previous page

Field	Label in UI	Type	Description
parser	Parser	String	Value must be one of the following: SyslogParser LineParser MultiLineSyslogParser ProofPointEmailProtectionLogParser EmailParser Mandatory only when the value of the proxy_condition parameter is "use_as_proxy" or "None". Optional Field
processpolicy	Processing Policy	String	Existing Processing Policy id or "None". Execute the ProcessingPolicy - List API to obtain the value of the required Processing Policy id . Mandatory only when the value of 'proxy_condition' is "uses_proxy" or "None". Optional Field
proxy_condition	Proxy Server	String	Value can be "uses_proxy", "use_as_proxy" or "None". Mandatory Field
proxy_ip	Proxy IP	[String]	List of IP address of the Proxy Server(s) where the value of the proxy_condition parameter is "uses_proxy". Optional Field

Request Example

```
{
   "data": {
      "hostname": [
         "Logpoint"
      ],
      "processpolicy": "57724aacd8aaa40b569bcb1fasd",
      "proxy_condition": "uses_proxy",
      "proxy_ip": [
         "1.1.1.1"
      ]
   }
}
```

Success Response

```
{
   "status": "Success",
```

(continues on next page)

(continued from previous page)

```
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

51.3 SyslogCollector - Trash

Deletes the Syslog Collector with given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SyslogCollector/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	UUID of the respective SyslogCollector. To obtain the Syslog collector uuid , execute Devices - List API if the collector was configured using device id or execute LogCollectionPolicies - List API if the collector was configured using log collection policy id . Mandatory Field

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

FIFTYTWO

SYSTEMSETTINGSENRICHMENT

52.1 SystemSettingsEnrichment - List

Lists the current Enrichment System Settings List.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪SystemSettingsEnrichment
```

Success Response

```
[
  {
    "clients_map": {},
    "enrich_mode": null,
    "forwarders_map": {},
    "id": "5943684cd8aaa4770455df34",
    "is_forwarder": false,
    "is_standalone": true,
    "private_ip": "",
    "remote_ip": "192.168.1.4",
    "subscription_sources": [
      {
        "logpoint_identifier": "b82b60f63cb04e21b8782da16814ed07",
        "text": "LogPoint192 ( 10.45.1.192)",
        "value": "10.85.128.1"
      },
      {
        "logpoint_identifier": "ef803a513f5441d6b00b17810d39c140",
        "text": "LogPoint191 ( 10.45.1.191)",
        "value": "10.210.52.1"
      }
    ]
  }
]
```

52.2 SystemSettingsEnrichment - RefreshList

Syncs the current Enrichment System Settings List with LogPoint's Enrichment System Settings List.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪SystemSettingsEnrichment/refreshlist
```

Request Example

```
{
    "data": {}
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

52.3 SystemSettingsEnrichment - Save

Updates the existing Enrichment System Settings.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪SystemSettingsEnrichment
```

Parameter

Field	Label in UI	Type	Description
enrich_mode	Enrichment Propagation	String	Enrich mode value can be one of the following: source: Enrichment Provider. Collects and Shares the content of the Enrichment Source with Client LogPoints. client: Enrichment Subscriber. Receives the Enrichment Data from the Source machine. Mandatory only when the value of the standalone parameter is "off". Optional Field
remote_ip	Subscription source	String	Remote source IP. Use the value of the required subscription source IP from SystemSettingsEnrichment - List API. Mandatory only when the value of the enrich_mode parameter is "client". Optional Field
standalone	Standalone Mode	String	Values can be: on - Standalone Mode off - Distributed Mode. Mandatory Field

Request Example

```
{
   "data": {
      "enrich_mode": "source",
      "remote_ip": "192.168.4.32",
      "standalone": "on"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

FIFTYTHREE

SYSTEMSETTINGSGENERAL

53.1 SystemSettingsGeneral - List

Lists all General System Settings.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪SystemSettingsGeneral
```

Success Response

```
[
  {
    "auth_ldap": false,
    "auth_li": true,
    "buffering": false,
    "default_auth": "LogpointAuthentication",
    "default_ha_path": "/opt/immune/storage",
    "enable_soar": true,
    "id": "591ec024d8aaa45be61fab2c",
    "identifier": "3f6d4866f6f6437eaf0737869ad948a2",
    "ip_dns": "10.232.21.1",
    "is_msui": false,
    "lp_mode": "search_head",
    "name": "LogpointMain",
    "overscan_period": 1.0,
    "sequence_number": false,
    "share_usage_data": false,
    "tab_title": "Logpoint",
    "timeout": 30,
    "timestamp_on": "col_ts",
    "timezone": "Asia/Kathmandu",
    "type": "installation"
  }
]
```

53.2 SystemSettingsGeneral - ListAuth

Lists all available authentication types for Logpoint.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪SystemSettingsGeneral/auth
```

Success Response

```
[
    {
        "name": "LogpointAuthentication",
        "text": "Logpoint Authentication"
    },
    {
        "name": "LDAPAuthentication",
        "text": "LDAP Authentication"
    }
]
```

53.3 SystemSettingsGeneral - RefreshAuthList

Syncs the list of the available authentication types for Logpoint.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪SystemSettingsGeneral/refreshAuthlist
```

Request Example

```
{
    "data": {}
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

53.4 SystemSettingsGeneral - Save

Updates the existing General System Settings.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪SystemSettingsGeneral
```

Parameter

Field	Label in UI	Type	Description
default_auth	Default Login Screen From	String	Default Logpoint authentiation type. Obtain the value of the required authentication type name using **SystemSettingsGeneral - ListAuth API**. Mandatory Field.
default_ha_path	Path	String	Default High-Availability repo path. Mandatory Field.
enable_soar	SOAR	boolean	Enable or disable SOAR. Value can be “true” or “false”. Value will be retained in absence of the *enable_soar* parameter in the request. Optional Field.
li_ip	Server Alias	String	Logpoint IP address. Mandatory Field.
lp_mode	Modes	String	Mode of logpoint. Possible values are “search_head” and “dlp”. Mandatory Field.
name	Logpoint Name	String	Logpoint name. Mandatory Field.
overscan_period	Over Scan Period (in minutes)	int	Overscan period. Mandatory Field.
share_usage_data	Share Usage Data	boolean	Shares user’s usage data with Logpoint. Value can be “true” or “false”. The default value is “false”. Set the value to “true” to share the usage data. Optional Field.
tab_title	Browser tab title	String	Tab title for the Logpoint. Optional Field.

Continued on next page

Table 1 – continued from previous page

Field	Label in UI	Type	Description
timeout	Timeout (minutes)	int	Idle timeout for the session. Mandatory Field.
timestamp_on	Apply Time Range On	String	Timestamp to index the logs. Possible values are 'log_ts' and 'col_ts'. Mandatory Field.
timezone	Time Zone	String	One of the timezones given by Logpoint. Obtain the available timezones using **Timezone - List API**. Mandatory Field.

Request Example

```
{
   "data": {
      "default_auth": "LogpointAuthentication",
      "default_ha_path": "/opt/immune/storage",
      "enable_soar": "true",
      "li_ip": "192.168.0.0",
      "lp_mode": "search_head",
      "name": "LogpointTest",
      "overscan_period": 1,
      "share_usage_data": "true",
      "tab_title": "MyLogpoint",
      "timeout": 30,
      "timestamp_on": "col_ts",
      "timezone": "Asia/Kathmandu"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

FIFTYFOUR

SYSTEMSETTINGSHTTPS

54.1 SystemSettingsHTTPS - InstallCertificate

Install the certificate and key in the provided logpoint

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪SystemSettingsHTTPS/certificate/install
```

Parameter

Field	Label in UI	Type	Description
certificate	Certificate	String	Name of the certificate file to install. Mandatory Field
file_location	-	String	Location of the file to install. Can be either 'private' or 'public'. Mandatory Field
key	Key	String	Name of the key file to install. Mandatory Field

Request Example

```
{
   "data": {
      "certificate": "ssl.crt",
      "file_location": "private",
      "key": "ssl.key"
   }
}
```

Success Response

```
{
```

(continues on next page)

(continued from previous page)

```
    "status": "Success",
    "message": "/monitorapi/v1/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

54.2 SystemSettingsHTTPS - List

List all the keys and certificate in private storage for the requested pool

GET

```
https://api-server-host-name/configapi/{pool_UUID}/SystemSettingsHTTPS/list
```

Success Response

```
[
    "ssl.key",
    "ssl.crt"
]
```

54.3 SystemSettingsHTTPS - ListPublic

List all the keys and certificate in public storage

GET

```
https://api-server-host-name/configapi/SystemSettingsHTTPS/list
```

Success Response

```
[
    "ssl.key",
    "ssl.crt"
]
```

54.4 SystemSettingsHTTPS - TrashPrivate

Delete the file with given name from private storage

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/SystemSettingsHTTPS/{file_name}
```

Parameter

Field	Label in UI	Type	Description
file_name		String	File to be deleted. Mandatory Field

Success Response

```
{
    "status": "Success",
    "message": "ssl.crt successfully deleted"
}
```

54.5 SystemSettingsHTTPS - TrashPublic

Delete the file with given name from public storage

DELETE

```
https://api-server-host-name/configapi/SystemSettingsHTTPS/{file_name}
```

Parameter

Field	Label in UI	Type	Description
file_name		String	File to be deleted. Mandatory Field

Success Response

```
{
    "status": "Success",
    "message": "ssl.key successfully deleted"
}
```

54.6 SystemSettingsHTTPS - UploadCertificate

Upload certificate and key to public storage

POST

```
https://api-server-host-name/configapi/SystemSettingsHTTPS/certificate
```

Header

Field	Label in UI	Description
Content-Type		multipart/form-data
replace_existing		Set the value of this parameter as 'true' to replace the existing file with the same name with the new file. Default value is 'false'. Value can be 'true' or 'false'. Optional field

Parameter

Field	Label in UI	Type	Description
certificate	Certificate	[Object]	ssl certificate to be uploaded. Mandatory Field
key	Key	[Object]	ssl key to be uploaded. Mandatory Field

Success Response

```
{
    "status": "Success",
    "message": "Certificate and key successfully uploaded"
}
```

54.7 SystemSettingsHTTPS - UploadCertificateToPool

Upload certificate and key to private storage

POST

```
https://api-server-host-name/configapi/{pool_UUID}/SystemSettingsHTTPS/certificate
```

Header

Field	Label in UI	Description
Content-Type		multipart/form-data
replace_existing		Set the value of this parameter as 'true' to replace the existing file with the same name with the new file. Default value is 'false'. Value can be 'true' or 'false'. Optional field

Parameter

Field	Label in UI	Type	Description
certificate	Certificate	[Object]	ssl certificate to be uploaded. Mandatory Field
key	Key	[Object]	ssl key to be uploaded. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "Certificate and key successfully uploaded"
}
```

CHAPTER

FIFTYFIVE

SYSTEMSETTINGSLOCKOUTPOLICY

55.1 SystemSettingsLockoutPolicy - List

Lists the Lockout policy Settings.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪SystemSettingsLockoutPolicy
```

Success Response

```
[
    {
        "failed_login": 7,
        "id": "4f031d6bccba252fb00fbf61",
        "locked_out_time": 20
    }
]
```

55.2 SystemSettingsLockoutPolicy - PolicyReset

Resets the Lockout policy parameters to default values. The default value for locked_out_time is 30 minutes and the default value for the failed_login is 5.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪SystemSettingsLockoutPolicy/policyreset
```

Request Example

```
{
    "data": {}
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

55.3 SystemSettingsLockoutPolicy - Save

Updates the existing Lockout policy Settings.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪SystemSettingsLockoutPolicy
```

Parameter

Field	Label in UI	Type	Description
failed_login	Lockout threshold	int	Number of failed attempts at logon a user is allowed before the account is locked out. Default value is 5. Mandatory Field
locked_out_time	Lockout duration	int	Time in minutes that the account can be locked out. Default value is 30. Mandatory Field

Request Example

```
{
   "data": {
      "failed_login": 5,
      "locked_out_time": 30
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

FIFTYSIX

SYSTEMSETTINGSMODESOFOPERATION

56.1 SystemSettingsModesOfOperation - List

Lists the modes of operations available.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪SystemSettingsModesOfOperation
```

Success Response

```
[
    {
        "buffering": false,
        "is_li_light": true,
        "remote_li": ""
    }
]
```

56.2 SystemSettingsModesOfOperation - Save

Configures the Fabric-enabled LogPoint as a LogPoint Collector.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪SystemSettingsModesOfOperation
```

Parameter

Field	Label in UI	Type	Description
buffering	Enable Buffering	String	Accepts value as "on" or "off" to enable or disable buffering when the value of is_li_lite parameter is set as "on". Enabling buffering stores data in local persistent storage during network outage. Optional Field
is_li_lite	Is this a LogPoint Collector installation?	String	Set the values of this parameter as "on" or "off" to enable or disable your LogPoint as a LogPoint Collector. Mandatory Field

Request Example

```
{
   "data": {
      "buffering": "on",
      "is_li_lite": "on"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

FIFTYSEVEN

SYSTEMSETTINGSNTP

57.1 SystemSettingsNTP - List

Lists the NTP System Settings.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SystemSettingsNTP
```

Success Response

```
[
    {
        "changed": false,
        "id": "59147407d8aaa45c67a77d54",
        "ntp_enabled": false,
        "ntp_server": [
            "ntp.ubuntu.com",
            "test.domain.com",
            "ntp.logpoint.com"
        ]
    }
]
```

57.2 SystemSettingsNTP - NTPRestart

Restarts the NTP Server, if it is already enabled.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SystemSettingsNTP/
↪ntprestart
```

Request Example

```
{
    "data": {}
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

57.3 SystemSettingsNTP - Save

Updates the existing NTP System Settings.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SystemSettingsNTP
```

Parameter

Field	Label in UI	Type	Description
ntp_enabled	Is NTP enabled?	String	Value must be "on" to enable NTP Server. Optional Field
ntp_server	Server	[String]	List of the NTP Server(s) that must be enabled. Mandatory only when the value of ntp_enabled parameter is "on". Mandatory Field

Request Example

```
{
    "data": {
        "ntp_enabled": "on",
        "ntp_server": [
            "ntp.ubuntu.com",
            "ntp.logpoint.com"
        ]
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

FIFTYEIGHT

SYSTEMSETTINGSSMTP

58.1 SystemSettingsSMTP - List

Lists all SMTP System Settings.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SystemSettingsSMTP
```

Success Response

```
[
    {
        "id": "59193916d8aaa438912a79a6",
        "login_required": true,
        "smtp_port": 25,
        "smtp_sender_email": "john_doe1@domain.com",
        "smtp_sender_name": "John Doe",
        "smtp_server": "192.168.1.34",
        "smtp_username": "logpointnepal@gmail.com",
        "username_in_email_field": ""
    }
]
```

58.2 SystemSettingsSMTP - SMTPTest

Tests SMTP Settings.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SystemSettingsSMTP/
↪smtptest
```

Parameter

Field	Label in UI	Type	Description
email	Email	String	Receiver's Email address. Mandatory Field
login_required	Login Required	String	Value must be "on" if login is mandatory for sending email from the given address. Optional Field
message	Message	String	Body of the Email. Mandatory Field
smtp_password	Password	String	Password for authentication. Mandatory only when the value of the login_required parameter is "on". Optional Field
smtp_port	Port	int	SMTP Server Port number. Default Value = 25. Optional Field
smtp_sender_email	Email	String	Sender's Name. Mandatory Field
smtp_server	Server	String	Hostname or IP Address of the SMTP Server. Mandatory Field
smtp_username	Username	String	Username for authentication. Mandatory only when the value of the login_required parameter is "on". Optional Field
subject	Subject	String	Subject of the Email. Mandatory Field

Request Example

```
{
   "data": {
      "email": "ram@logpoint.com",
      "login_required": "on",
      "message": "This is a test",
      "smtp_password": "ram",
      "smtp_port": 25,
      "smtp_sender_email": "ram@logpoint.com",
      "smtp_server": "192.168.1.34",
      "smtp_username": "ram",
      "subject": "SMTP configuration test"
   }
}
```

Success Response

```
{
```

(continues on next page)

(continued from previous page)

```
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

58.3 SystemSettingsSMTP - Save

Updates the existing SMTP System Settings.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SystemSettingsSMTP
```

Parameter

Field	Label in UI	Type	Description
login_required	Login Required	String	Value must be "on" if login is mandatory for sending email from the given address. Optional Field
smtp_password	Password	String	Password for authentication. Mandatory only when the value of the login_required parameter is "on". Optional Field
smtp_port	Port	int	SMTP Server Port number. Default Value = 25. Optional Field
smtp_sender_email	Email	String	Sender's Email. Mandatory Field
smtp_sender_name	Sender Name	String	Sender's Name. Mandatory Field
smtp_server	Server	String	Hostname or IP Address of the SMTP Server. Mandatory Field
smtp_username	Username	String	Username for authentication. Mandatory only when the value of the login_required parameter is "on". Optional Field

Request Example

```
{
    "data": {
        "login_required": "on",
        "smtp_password": "ram",
        "smtp_port": 25,
```

(continues on next page)

(continued from previous page)

```
        "smtp_sender_email": "ram@logpoint.com",
        "smtp_sender_name": "ram",
        "smtp_server": "192.168.1.34",
        "smtp_username": "ram"
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

FIFTYNINE

SYSTEMSETTINGSSNMP

59.1 SystemSettingsSNMP - List

Lists all SNMP System Settings.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SystemSettingsSNMP
```

Success Response

```
[
   {
      "community_string": "test",
      "id": "591a8b3dd8aaa438912a79a7",
      "public_string": "public",
      "snmpd_enabled": true
   }
]
```

59.2 SystemSettingsSNMP - Save

Updates the existing SNMP System Settings.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SystemSettingsSNMP
```

Parameter

Field	Label in UI	Type	Description
community_string	Community String	String	The community string for authentication in SNMP v2. Mandatory only when the value of the "snmpd_access" parameter is 'true'. Optional Field
snmpd_access	SNMPD Port (UDP 161)	boolean	Value must be "true" if login is mandatory for sending email from the given address. Mandatory Field

Request Example

```
{
   "data": {
      "community_string": "public",
      "snmpd_access": "true"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

SIXTY

SYSTEMSETTINGSSSH

60.1 SystemSettingsSSH - List

Lists all SSH Key-pairs System Settings.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SystemSettingsSSH
```

Success Response

```
[
  {
    "private_key": "-----BEGIN RSA PRIVATE KEY-----\nProc-Type4,ENCRYPTED\nDEK-InfoAES-
↪128-CBC,E0A19FA913F080388D71DFDB80B4AA70\n\nH/
↪sy90okqei7dfpLaylkoLAMArIRshaMntZizBO8Lm+y1wi5OXU4Q3RyyZwc7\nkL5jqKwpNaYAkyq4cPSrq1sk4DRk8
↪oKxaJyM6NdlKcip0YuLeVgmri2zpuFhTf7FRhUEfQ21gJ\n/
↪wTni+gQFiwuFna3TOJoK+k1PboXkxtLH2qkNDmgHdcligkW4j9e0Ci9zZRjqZ6A\ng8nv+Fw4Jx+ezSZjhJTIGTIN
↪7JPPQpFgMiOJAC7ie9BjeScjuxANHKftlA\n6JHEtCUpsUn3OH6HOs/
↪SsDqNz2fZumYxzLzZe7ldIFEtxEGM6TB7cEkgEskpkLhK\nnRkfqnXMADsYKK9IFmxEXn0AK0dcNdUTjabfFNCjL
↪Ypy/9I/
↪QGTrRVYW9YtKyPuM9QiI92YgvTr6QALCUMMD+hmKzZi5ZtU5XbZ\nVTF9co12w68HghazxyjgqLJIWsnXic4e5h
↪ne/2uEVHbUPekaX331OzyX2B2vtAuLlkWOrBKmK5T/uZKG\nSB6yY7h9QC1KRCNceZ/
↪f20CDDn8sobIC9wUpl3zLJ0xks5xihrlDFTJK0wjAIbOV\nmJWvmi6nVr4nssCzXGXuHOcB+4drEarScJSRI/
↪9fT7kj3DTTiORusiUzDSXQJ5AU\nWBkAY9t66eaXZxW17PgE7AZroGBfTkO2gplfmlGz0xdaMvQy/
↪Cp30qyh4qKWM5VF\nJBTET3OgiyBPkKUeAHyUCUJDRSwnak7bVe3qztzjSQd4+qKDDahD5/
↪I9uAJ5Hnqt\nB35StmtD/
↪QPo+Cm+aTuwnneyv87fMv3VAzWZtJpyJAvnnj+QRJi4r6tkyHEgVA3+\nTL0WhUqijA00JKQGOmJ61NLq8YKD
↪nXkYHjn6mlnBENPrtjjTvHurVAbXDBFZNf4Wh1v22gdQVRCIAKyk3lE23KRv\n/AZ3kaq2Oq/
↪pVX0Ph13SJNoOn0Ds8S4SDLROzlq7nOUQMRqhG1OyiUbAgizR9MVw\nHUmKPj99QouUsZN5UfBSojP6R6giZ
↪CDS88Zo7rshRs0BfQt7n\nd9td8bDbUC2IAdMIVPKw0bqHc3jB/
↪ixSCNivZ962AapB9WpP5Srw9bZnoLj7dxdm\nKkB/
↪GCsqjUqO80pCzhtvuw2RCuyBE6IHOBoij3+wq2VIcwvy1fr81pA1QLnzB2g2\nNQ7KgVypsKP2Dref0D5chtKqIzV
↪MRv8kXIioJ6zwBLB/yfaY\n-----END RSA PRIVATE KEY-----\n"
  }
]
```

60.2 SystemSettingsSSH - Save

Updates the existing SSH Key-pair System Settings.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SystemSettingsSSH
```

Parameter

Field	Label in UI	Type	Description
pass_phrase	Pass Phrase	String	Passphrase for creating a private key. Mandatory Field

Request Example

```
{
   "data": {
      "pass_phrase": "abcdef"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

SIXTYONE

SYSTEMSETTINGSSUPPORTCONNECTION

61.1 SystemSettingsSupportConnection - List

Lists all Support Connection settings.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪SystemSettingsSupportConnection
```

Success Response

```
[
    {
        "connection_forever": false,
        "enable_days": 5,
        "enable_hours": 3,
        "enable_minutes": 58,
        "support_connection": true,
        "support_connection_ip": "10.99.0.7"
    }
]
```

61.2 SystemSettingsSupportConnection - RefreshList

Syncs the current Support Connection Settings list with LogPoint's Support Connection settings.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪SystemSettingsSupportConnection/refreshlist
```

Request Example

```
{
    "data": {}
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

61.3 SystemSettingsSupportConnection - Save

Updates the existing settings of Support Connection.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/
↪SystemSettingsSupportConnection
```

Parameter

Field	Label in UI	Type	Description
connection_forever	Enable Support Connection Forever	boolean	Value must be "true" to enable Support Connection forever. Default Value: "false". Optional Field
enable_days	Days	int	Time limit in days to keep support connection active. Mandatory only when the value of the connection_forever parameter is "false". Optional Field
enable_hours	Hours	int	Time limit in hours to keep support connection active. Mandatory only when the value of the connection_forever parameter is "false". Optional Field

Continued on next page

Table 1 – continued from previous page

Field	Label in UI	Type	Description
enable_minutes	Minutes	int	Time limit in minutes to keep support connection active. Mandatory only when the value of the connection_forever parameter is "false". Optional Field
support_connection	Enable Support Connection	String	Value must be "on" to enable Support Connection. Optional Field

Request Example

```
{
   "data": {
      "connection_forever": "true",
      "enable_days": 1,
      "enable_hours": 0,
      "enable_minutes": 0,
      "support_connection": "on"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

SIXTYTWO

SYSTEMSETTINGSSYSLOG

62.1 SystemSettingsSyslog - InstallCertificate

Installs the certificate and key in the selected Logpoint and updates Syslog settings.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SystemSettingsSyslog/
↪certificate/install
```

Parameter

Field	Label in UI	Type	Description
certificate	Certificate	String	Name of the certificate file to install. Mandatory only when the value of the key is present in the request. Optional Field.
file_location	-	String	Location of the file to install. Can be either 'private' or 'public'. Mandatory only when the value of the key and the certificate is present in the request. Optional Field.
key	Key	String	Name of the key file to install. Mandatory only when the value of the certificate is present in the request. Optional Field.
sequence_number	Sequence Numbering	boolean	Flag for adding sequence numbers to the log received from the Syslog Collector. Value can be 'true' or 'false'. Optional Field.

Continued on next page

Table 1 – continued from previous page

Field	Label in UI	Type	Description
syslog_max_log_size_kb	Message Length	int	Maximum possible length of a syslog message in kb. Default value is 12kb. Minimum value is 1kb and it's value cannot be greater than 64 kb. Optional Field.

Request Example

```
{
   "data": {
      "certificate": "client.crt",
      "file_location": "public",
      "key": "client.key",
      "sequence_number": "true",
      "syslog_max_log_size_kb": 7
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/v1/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

62.2 SystemSettingsSyslog - List

List all the keys and certificates in private storage for the requested pool.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/SystemSettingsSyslog/list
```

Success Response

```
[
   "client.key",
   "client.crt"
]
```

62.3 SystemSettingsSyslog - ListPublic

List all the keys and certificates in public storage.

GET

```
https://api-server-host-name/configapi/SystemSettingsSyslog/list
```

Success Response

```
[
  "client.key",
  "client.crt"
]
```

62.4 SystemSettingsSyslog - ListSyslogSettings

Lists current syslog settings

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/SystemSettingsSyslog
```

Success Response

```
[
  {
    "certificate_status": {
      "organization": "MGO",
      "server_name": false,
      "status": "MGO Certificates have already been installed"
    },
    "sequence_number": true,
    "syslog_max_log_size_kb": 8
  }
]
```

62.5 SystemSettingsSyslog - TrashPrivate

Deletes the file with the provided name from private storage.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/SystemSettingsSyslog/{file_name}
```

Parameter

Field	Label in UI	Type	Description
file_name		String	File to be deleted. Mandatory Field.

Success Response

```
{
    "status": "Success",
    "message": "client.crt successfully deleted"
}
```

62.6 SystemSettingsSyslog - TrashPublic

Deletes the file with the provided name from public storage.

DELETE

```
https://api-server-host-name/configapi/SystemSettingsSyslog/{file_name}
```

Parameter

Field	Label in UI	Type	Description
file_name		String	File to be deleted. Mandatory Field.

Success Response

```
{
    "status": "Success",
    "message": "client.key successfully deleted"
}
```

62.7 SystemSettingsSyslog - UploadCertificate

Uploads the certificate and the key to public storage.

POST

```
https://api-server-host-name/configapi/SystemSettingsSyslog/certificate
```

Header

Field	Label in UI	Description
Content-Type		multipart/form-data
replace_existing		Change the parameter value to 'true' to replace the existing file with a new one with the same name. Default value is 'false'. Value can only be 'true' or 'false'. Optional field.

Parameter

Field	Label in UI	Type	Description
certificate	Certificate	[Object]	ssl certificate to be uploaded. Mandatory Field.
key	Key	[Object]	ssl key to be uploaded. Mandatory Field.

Success Response

```
{
   "status": "Success",
   "message": "Certificate and key successfully uploaded"
}
```

62.8 SystemSettingsSyslog - UploadCertificateToPool

Uploads the certificate and the key to private storage.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/SystemSettingsSyslog/certificate
```

Header

Field	Label in UI	Description
Content-Type		multipart/form-data
replace_existing		Change the parameter value to 'true' to replace the existing file with a new one with the same name. Default value is 'false'. Value can only be 'true' or 'false'. Optional field.

Parameter

Field	Label in UI	Type	Description
certificate	Certificate	[Object]	ssl certificate to be uploaded. Mandatory Field.
key	Key	[Object]	ssl key to be uploaded. Mandatory Field.

Success Response

```
{
   "status": "Success",
   "message": "Certificate and key successfully uploaded"
}
```

CHAPTER

SIXTYTHREE

TABLES

63.1 Tables - Create

Creates a dynamic table that stores the specified field and field values synchronously during the runtime for a limited or an unlimited period of time.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Tables
```

Parameter

Field	Label in UI	Type	Description
agelimit_day	Day	int	Expiration time for the values in the table. The values expire after the specified age limit. The value of the parameter must be in days and the maximum value should not be more than 9999 days. Mandatory Field.
agelimit_hour	Hour	int	Specify the value of the age limit in hours. The maximum value for this field is 23. Mandatory Field.
agelimit_minute	Minute	int	Specify the value of the age limit in minutes. The maximum value for this field is 59. The age limit must be at least 30 or 0 minutes. If you do not want the values to expire, set the age limit to 0. Mandatory Field.

Continued on next page

Table 1 – continued from previous page

Field	Label in UI	Type	Description
source_name	Name	String	Specify the name for the table which is automatically represented in uppercase. The value can be alphanumeric characters with underscore(_) and the value should not begin or end with white space character and hyphen(-). Mandatory Field.

Request Example

```
{
   "data": {
      "agelimit_day": 4,
      "agelimit_hour": 5,
      "agelimit_minute": 39,
      "source_name": "TABLE"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

63.2 Tables - Edit

Updates a dynamic table that stores the specified field and field values during the runtime for a limited or an unlimited period of time with given ID.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Tables/{id}
```

Parameter

Field	Label in UI	Type	Description
agelimit_day	Day	int	Expiration time for the values in the table. The values expire after the specified age limit. The value of the parameter must be in days and the maximum value should not be more than 9999 days. Mandatory Field.
agelimit_hour	Hour	int	Specify the value of the age limit in hours. The maximum value for this field is 23. Mandatory Field.
agelimit_minute	Minute	int	Specify the value of the age limit in minutes. The maximum value for this field is 59. The age limit must be at least 30 or 0 minutes. If you do not want the values to expire, set the age limit to 0. Mandatory Field.
id	-	String	Existing table ID. Mandatory Field.

Request Example

```
{
   "data": {
      "agelimit_day": 4,
      "agelimit_hour": 5,
      "agelimit_minute": 39
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

63.3 Tables - Get

Fetches a single dynamic table with given ID.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Tables/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing table ID. Obtain the current data of tables with Logpoint's tables using **EnrichmentSource-RefreshList**.

Success Response

```
{
    "active": true,
    "age_limit": 365940,
    "delete_status": "",
    "id": "634e3c347d022ec4084f8d83",
    "last_updated": 1666071858,
    "plugin_info": {
        "enrichment_options": {
            "age_limit": 365940
        },
        "source_fields": [
            {
                "field": "device_ip",
                "type": "IP"
            },
            {
                "field": "norm_id",
                "type": "string"
            }
        ],
        "table_option": {
            "dynamictable_name": "DEVICE_IP_TABLE"
        }
    },
    "reason": null,
    "result": "Updated",
    "source_info": {
        "id": "a62b1ae1d316ba691fb7549bc4210e7f",
        "source_name": "dynamictable"
    },
    "source_name": "DEVICE_IP_TABLE",
    "source_type": "DynamicTable",
    "tid": ""
}
```

63.4 Tables - List

Lists all dynamic tables. Obtain the current data of tables with Logpoint's tables using **EnrichmentSource-RefreshList**.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Tables
```

Success Response

```
[
    {
        "active": true,
        "age_limit": 365940,
        "delete_status": "",
        "id": "634e3c347d022ec4084f8d83",
        "last_updated": 1666071858,
        "plugin_info": {
            "enrichment_options": {
                "age_limit": 365940
            },
            "source_fields": [
                {
                    "field": "device_ip",
                    "type": "IP"
                },
                {
                    "field": "norm_id",
                    "type": "string"
                }
            ],
            "table_option": {
                "dynamictable_name": "DEVICE_IP_TABLE"
            }
        },
        "reason": null,
        "result": "Updated",
        "source_info": {
            "id": "a62b1ae1d316ba691fb7549bc4210e7f",
            "source_name": "dynamictable"
        },
        "source_name": "DEVICE_IP_TABLE",
        "source_type": "DynamicTable",
        "tid": ""
    }
]
```

63.5 Tables - Trash

Deletes the dynamic table with the given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Tables/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing table ID. Mandatory Field.

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

CHAPTER

SIXTYFOUR

TIMEZONE

64.1 Timezone - List

Lists all Timezones available.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Timezone
```

Success Response

```
[
  {
    "description": "(GMT-11:00) Midway Island, Samoa",
    "name": "Pacific/Midway"
  },
  {
    "description": "(GMT-10:00) Hawaii-Aleutian",
    "name": "America/Adak"
  },
  {
    "description": "(GMT-10:00)Hawaii",
    "name": "Etc/GMT+10"
  },
  {
    "description": "(GMT-09:30) Marquesas Islands",
    "name": "Pacific/Marquesas"
  },
  {
    "description": "(GMT-09:00) Gambier Islands",
    "name": "Pacific/Gambier"
  }
]
```

CHAPTER

SIXTYFIVE

UEBA

65.1 UEBA - ConfigureAlertLogs

Configures the UEBA alerts risk score which is used to categorize the UEBA anomalies based on their risk level.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/UEBA/configureAlert
```

Parameter

Field	Label in UI	Type	Description
base_risk_check	ALERT LOGS CONFIGURATION	int	UEBA alert risk score. Value can be a number between 0 and 100. Default value is 75. LogPoint classifies the risk scores into four different types: • Low Risk Score Range: 00 to 25 • Medium Risk Score Range: 26 to 50 • High Risk Score Range: 51 to 75 • Extreme Risk Score Range: 76 to 100 Mandatory Field

Request Example

```
{
   "data": {
      "base_risk_check": 46
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

65.2 UEBA - ConfigureRepo

Adds the repositories for UEBA analysis. You can also enable the history service to forward 30 days of historical data to UEBA.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/UEBA/configureRepo
```

Parameter

Field	Label in UI	Type	Description
enable_history_service	Enable history service	boolean	Select this value as “true” to enable the history service to forward 30 days of historical data to UEBA. Default value is “true”. You can enable the history service only once. Select the value as “false” for LogPoint to forward input data from the date you configure the repos. Optional Field
include_all_repos	-	boolean	Set this value as “true” to select all the repos for UEBA configurations. Either “include_all_repos” with value “true” or non-empty “source_repos” must be present while configuring UEBA Repos. Optional Field

Continued on next page

Table 2 – continued from previous page

Field	Label in UI	Type	Description
source_repos	SELECT REPOS	[String]	Repositories of the LogPoint Search Head and Distributed LogPoints for UEBA analysis. Optional Field

Request Example

```
{
   "data": {
      "enable_history_service": "true",
      "source_repos": [
         "127.0.0.1:5504/_LogPointAlerts",
         "127.0.0.1:5504/_logpoint"
      ]
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

65.3 UEBA - CreateEntity

Adds new entities for UEBA analysis.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/UEBA/
↪UEBAEntitySelections
```

Parameter

Field	Label in UI	Type	Description
content_type	Content Type	String	It can have values as CIDR, IP or HOSTNAME. Mandatory only when machine is entity_type_rb is selected as Machine. Optional Field

Continued on next page

Table 3 – continued from previous page

Field	Label in UI	Type	Description
entity_group_name	CREATE ENTITY	String	The name of the entity group. Mandatory Field
entity_type_rb	Users/Machines	String	The type of the entities in the group. It can either be User or Machine. Mandatory Field
source_field_name	Select the field name that can uniquely identify Users	String	Field from the selected enrichment source that can uniquely identify each entity. Mandatory Field
source_name	Name	String	Name of the enrichment source used. Obtain the value of this parameter using EnrichmentSource - List API. Mandatory Field
source_type	Source Type	String	The type of the enrichment source used for entity selection. It can be LDAP, CSV, or ODBC. Mandatory Field
uebafiltering	Entities filtering	[json]	**Array of key-value pair objects to filter the en** • field_cb : Field from the selected enrichment source. • criteria_query : Query in the regex format. Optional Field
update_license_rg	Yes/No	boolean	Select True to update the selected entities every time the content of the enrichment source changes. Select False to never update the selected entities. Can have value as True or False only. Mandatory Field

Request Example

```
{
   "data": {
      "content_type": "CIDR",
      "entity_group_name": "entity1",
      "entity_type_rb": "Machine",
      "source_field_name": "device_ips",
      "source_name": "csv1",
      "source_type": "CSV",
      "uebafiltering": [
         {
            "criteria_query": "fabric",
            "field_cb": "device_name"
         }
      ],
      "update_license_rg": "true"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

65.4 UEBA - EditEntity

Edit the UEBA entities with the given ID.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/UEBA/
↪UEBAEntitySelections/{id}
```

Parameter

Field	Label in UI	Type	Description
content_type	Content Type	String	It can have values as CIDR, IP or HOSTNAME. Mandatory only when machine is *entity_type_rb* is selected as Machine. Optional Field

Continued on next page

Table 4 – continued from previous page

Field	Label in UI	Type	Description
entity_type_rb	Users/Machines	String	The type of the entities in the group. It can either be User or Machine. Mandatory Field
id	-	String	Entity id to edit. Mandatory Field
source_field_name	Select the field name that can uniquely identify Users	String	Field from the selected enrichment source that can uniquely identify each entity. Mandatory Field
source_name	Name	String	Name of the enrichment source used. Obtain the value of this parameter using EnrichmentSource - List API. Mandatory Field
source_type	Source Type	String	The type of the enrichment source used for entity selection. It can be LDAP, CSV, or ODBC. Mandatory Field
uebafiltering	Entities filtering	[json]	**Array of key-value pair objects to filter the en** • field_cb: Field from the selected enrichment source • criteria_query: Query in the regex format. Optional Field
update_license_rg	Yes/No	boolean	Select True to update the selected entities every time the content of the enrichment source changes. Select False to never update the selected entities. Can have value as True or False only. Mandatory Field

Request Example

```
{
```

(continues on next page)

(continued from previous page)

```
    "data": {
        "content_type": "CIDR",
        "entity_type_rb": "Machine",
        "source_field_name": "device_ips",
        "source_name": "csv1",
        "source_type": "CSV",
        "uebafiltering": [
            {
                "criteria_query": "fabric",
                "field_cb": "device_name"
            }
        ],
        "update_license_rg": "true"
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

65.5 UEBA - EnableUEBAMode

Enables or disables the UEBA configuration in the given LogPoint.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/UEBA/
↪UEBAConfigurations
```

Parameter

Field	Label in UI	Type	Description
enable_ueba_mode	ENABLE UEBA	boolean	Value of the parameter can be *true* or *false*. Setting this value as "true" sends request to enable UEBA and vice-versa. Mandatory Field

Request Example

```
{
    "data": {
        "enable_ueba_mode": "true"
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

65.6 UEBA - FetchHealthStatus

Fetches the health status and validation information of the UEBA.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/UEBA/UEBAHealth/
↪fetch
```

Request Example

```
{
    "data": {}
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}/{data_node}"
}
```

65.7 UEBA - FetchUEBALicenseState

Returns the details of UEBA License consumption in the given LogPoint.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/UEBA/
↪UEBALicenseInfo/fetch
```

Request Example

```
{
   "data": {}
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}/{data_node}"
}
```

65.8 UEBA - FetchValidationReport

Fetches the validation report of the UEBA.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/UEBA/
↪UEBAValidationReport/fetch
```

Request Example

```
{
   "data": {}
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}/{data_node}"
}
```

65.9 UEBA - GetEntity

Fetches the details of the UEBA entity with the given ID.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/UEBA/
↪UEBAEntitySelections/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing Entity id .

Success Response

```
{
   "id": "726a2e28880965cf253a18de",
   "info": {
      "entities_count": 15,
      "selection_updated": 1651126276,
      "status": "updated"
   },
   "priority": 1,
   "uebacreateentity": {
      "entity_group_name": "entityUser",
      "entity_type_rb": "User"
   },
   "uebafilterentity": {
      "source_field_name": "protocol",
      "update_license_rg": "true"
   },
   "uebaselectsource": {
      "source_name": "UEBA_ProtocolTable",
      "source_type": "CSV"
   }
}
```

65.10 UEBA - InstallUEBALicense

Installs the UEBA license.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/UEBA/install
```

Parameter

Field	Label in UI	Type	Description
confirm_override	-	String	Select this value as “yes” to install the UEBA license with a different client ID. Value can be yes/no. Default value is “yes”. Optional Field

Continued on next page

Table 7 – continued from previous page

Field	Label in UI	Type	Description
file_location	-	String	Location of fabric storage where the UEBA license is uploaded. Can be either 'private' or 'public'. Mandatory Field
file_name	-	String	Name of the pak file containing UEBA license. Mandatory Field

Request Example

```
{
   "data": {
      "confirm_override": "yes",
      "file_location": "private",
      "file_name": "license1.pak"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

65.11 UEBA - ListEntities

Returns a list of all the UEBA entities information.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/UEBA/
↪UEBAEntitySelections
```

Success Response

```
[
   {
      "id": "726a2e28880965cf253a18de",
      "info": {
         "entities_count": 15,
         "selection_updated": 1651126276,
         "status": "updated"
      },
```

(continues on next page)

(continued from previous page)

```
    "priority": 1,
    "uebacreateentity": {
      "entity_group_name": "entityUser",
      "entity_type_rb": "User"
    },
    "uebafilterentity": {
      "source_field_name": "protocol",
      "update_license_rg": "true"
    },
    "uebaselectsource": {
      "source_name": "UEBA_ProtocolTable",
      "source_type": "CSV"
    }
  }
]
```

65.12 UEBA - ListPrivateUploads

Lists the UEBA license package files available in the private storage.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/UEBA/list
```

Success Response

```
[
  "ueba.pak"
]
```

65.13 UEBA - ListPublicUploads

Lists the UEBA license package files available in public storage.

GET

```
https://api-server-host-name/configapi/UEBA/list
```

Success Response

```
[
  "ueba.pak"
]
```

65.14 UEBA - ListUEBAConfiguration

Lists all the UEBA configurations in the LogPoint.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/UEBA/
↪UEBAConfigurations
```

Success Response

```
[
    {
        "connector": null,
        "enable_ueba_mode": false,
        "first_repo_selected_ts": null,
        "history_service_status": null,
        "history_service_used": null,
        "id": "623d816e1151a0d03ee82c3f",
        "is_repo_selected": null,
        "licensed_entities_count": null,
        "mode": "master",
        "settings_valid": true,
        "source_repos": null,
        "source_repos_check": null,
        "status": "disabled",
        "streaming_server": null,
        "streaming_server_vpn_ip": null,
        "validity_period": null
    }
]
```

65.15 UEBA - ListUEBALicenseInfo

Lists the details of the UEBA license currently used in the given LogPoint.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/UEBA/UEBALicense
```

Success Response

```
[
    {
        "customer": {
```

(continues on next page)

(continued from previous page)

```
      "address1": "kathmandu",
      "address2": "",
      "name": "amrit",
      "phone": ""
    },
    "hardware_key": "00159-8FD3E-2801A-43049-DC859-9F297-6BA4D",
    "id": "523d8d7b1151a1d03ee72c42",
    "licensed_entities_count": "2600",
    "products": {
      "UEBA": {
        "id": "bc48ee12-caba-4844-b18e-d129f8640d74",
        "period": "2022/03/25-2028/10/03",
        "tenant_id": "q10"
      }
    }
  }
]
```

65.16 UEBA - RefreshUEBAConfigurationLists

Syncs the current UEBA Configuration List with LogPoint's Configuration List.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/UEBA/
↪UEBAConfigurations/refreshlist
```

Request Example

```
{
  "data": {}
}
```

Success Response

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

65.17 UEBA - RefreshUEBAEntityLists

Syncs the current UEBA Entity List with LogPoint's Entity List.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/UEBA/
↪UEBAEntitySelections/refreshlist
```

Request Example

```
{
   "data": {}
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

65.18 UEBA - TrashEntity

Delete a UEBA entity with the given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/UEBA/
↪UEBAEntitySelections/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	Existing entity ID. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

65.19 UEBA - TrashPrivateUploads

Deletes the UEBA license with the given name from private storage.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/UEBA/{file_name}
```

Parameter

Field	Label in UI	Type	Description
file_name		String	Name of the file to be deleted. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "ueba.pak successfully deleted"
}
```

65.20 UEBA - TrashPublicUploads

Deletes the UEBA license with the given name from public storage.

DELETE

```
https://api-server-host-name/configapi/UEBA/{file_name}
```

Parameter

Field	Label in UI	Type	Description
file_name		String	Name of the file to be deleted. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "ueba.pak successfully deleted"
}
```

65.21 UEBA - UpdateEntityPriorities

Updates the UEBA entities priorities.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/UEBA/updatePriorities
```

Parameter

Field	Label in UI	Type	Description
priorities	UPDATE PRIORITIES	[json]	Array of entity priorities where each object is a key-value pair of an entity and its priority. Each object in the array must include the following parameters: * name : Name of the entity * priority : Priority of the entity in number. 0 has the highest priority. The priority is used to discard an entity group when the selected entities exceed the number of licensed entities. By default, LogPoint prioritizes the entities on the basis of time they were added. Mandatory Field

Request Example

```
{
   "data": {
      "priorities": [
         {
            "name": "entity994",
            "priority": 0
         },
         {
            "name": "entity999",
            "priority": 1
         }
      ]
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

65.22 UEBA - Upload

Uploads UEBA license package files to private storage. This upload should be used for UEBA only.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/UEBA/upload
```

Header

Field	Label in UI	Description
file_name		Name of the file to be uploaded.
Content-Type		application/octet-stream
replace_existing		Set the value of this parameter as 'true' to replace the existing file with the same name with the new file. Default value is 'false'. Value can be 'true' or 'false'. Optional field

Parameter

Field	Label in UI	Type	Description
file	-	[Object]	(pak) to be uploaded. Mandatory Field

Success Response

```
{
    "status": "Success",
    "message": "ueba1.pak successfully uploaded in private storage. "
}
```

65.23 UEBA - UploadPublic

Uploads UEBA license package files to public storage. This upload should be used for UEBA only.

POST

```
https://api-server-host-name/configapi/UEBA/publicupload
```

Header

Field	Label in UI	Description
file_name		Name of the file to be uploaded.
Content-Type		application/octet-stream
replace_existing		Set the value of this parameter as 'true' to replace the existing file with the same name. Default value is 'false'. Optional field

Parameter

Field	Label in UI	Type	Description
file	-	[Object]	(pak) to be uploaded. Mandatory Field

Success Response

```
{
    "status": "Success",
    "message": "ueba1.pak successfully uploaded in public storage."
}
```

CHAPTER

SIXTYSIX

UPLOAD

66.1 Upload - Install

Install a given application

POST

```
https://api-server-host-name/configapi/Uploads/{pool_UUID}/{logpoint_identifier}/install
```

Parameter

Field	Label in UI	Type	Description
application_type	-	String	Type of the application to install. can be either 'application' or 'patch'. Mandatory Field
file_location	-	String	Location of the file to install. can be either 'private' or 'public'. Mandatory Field
file_name	File	String	Name of the file to install. Mandatory Field

Request Example

```
{
   "data": {
      "application_type": "Application",
      "file_location": "private",
      "file_name": "test_1.0.0.pak"
   }
}
```

Success Response

```
{
```

(continues on next page)

(continued from previous page)

```
    "status": "Success",
    "message": "/monitorapi/v1/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

66.2 Upload - List

List all files in private storage

GET

```
https://api-server-host-name/configapi/Uploads/{pool_UUID}/list
```

Success Response

```
[
    "test_1.0.0.pak"
]
```

66.3 Upload - ListPublic

List all files in public storage

GET

```
https://api-server-host-name/configapi/Uploads/list
```

Success Response

```
[
    "test_1.0.0.pak"
]
```

66.4 Upload - TrashPrivate

Delete the file with given name from private storage

DELETE

```
https://api-server-host-name/configapi/Uploads/{pool_UUID}/{file_name}
```

Parameter

Field	Label in UI	Type	Description
file_name		String	File to be deleted. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "test_1.0.0.pak successfully deleted"
}
```

66.5 Upload - TrashPublic

Delete the file with given name from public storage

DELETE

```
https://api-server-host-name/configapi/Uploads/{file_name}
```

Parameter

Field	Label in UI	Type	Description
file_name		String	File to be deleted. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "test_1.0.0.pak successfully deleted"
}
```

66.6 Upload - Upload

Upload files to private storage

POST

```
https://api-server-host-name/configapi/Uploads/{pool_UUID}
```

Header

Field	Label in UI	Description
file_name		Name of the file to be uploaded. The file name must be in the format name_version.pak.
Content-Type		application/octet-stream
replace_existing		Set the value of this parameter as 'true' to replace the existing file with the same name with the new file. Default value is 'false'. Value can be 'true' or 'false'. Optional field

Parameter

Field	Label in UI	Type	Description
file	-	[Object]	(Pak) to be uploaded. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "test_1.0.0.pak successfully uploaded in private storage. "
}
```

66.7 Upload - UploadPublic files

Upload files to public storage

POST

```
https://api-server-host-name/configapi/Uploads/PublicUpload
```

Header

Field	Label in UI	Description
file_name		Name of the file to be uploaded. The file name must be in the format name_version.pak.
Content-Type		application/octet-stream
replace_existing		Set the value of this parameter as 'true' to replace the existing file with the same name with the new file. Default value is 'false'. Value can be 'true' or 'false'. Optional field

Parameter

Field	Label in UI	Type	Description
file	-	[Object]	(Pak) to be uploaded. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "test_1.0.0.pak successfully uploaded in public storage. "
}
```

CHAPTER

SIXTYSEVEN

USERGROUPS

67.1 UserGroups - Create

Creates a new user group in a Fabric-enabled LogPoint.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/UserGroups
```

Parameter

Field	Label in UI	Type	Description
description	Description	String	Description of usergroup. Optional Field
name	Name	String	Name of usergroup. Mandatory Field

Continued on next page

Table 1 – continued from previous page

Field	Label in UI	Type	Description
object_permission	Object Permission	json	Mandatory Field. Specify permission for repos, usergroups, devices and ips. The following parameters should be provided to define object_permission. **include_all_permission**: Specifies full permission for repos and device_groups for all logpoints. If include_all_permission key is set as true, user should not give permission parameter in object_permission json. **permission**: List of jsons. To define permission, the following parameters should be provided. • *logpoint_ip*: Private IP of the logpoint. Use DistributedLogpoints - List API to obtain the private_ip of the required distributed logpoints. For localhost the logpoint_ip value is "127.0.0.1". Mandatory Field. • *include_all_repos*: Select/Unselect all repos for the given logpoint. If include_all_repos key is set as true, user should not give repos parameter. • *repos*: Name of the repos. Use Repos - FetchRemoteRepos API to obtain the names of the repos.

Table 1 – continued from previous page

Field	Label in UI	Type	Description
query	Universal Query	String	Universal Query for a user group. Optional Field
roles	Permission Group	String	Permission group. Mandatory Field

Request Example

```
{
    "data": {
        "description": "New usergroup",
        "name": "usergroup1",
        "object_permission": {
            "include_all_permission": false,
            "permission": [
                {
                    "include_all_device_groups": true,
                    "include_all_repos": true,
                    "logpoint_ip": "10.45.1.1"
                },
                {
                    "device_groups": [
                        {
                            "include_all_devices": true,
                            "name": "devicegroup3"
                        },
                        {
                            "devices": [
                                {
                                    "include_all_ips": true,
                                    "name": "device2"
                                }
                            ],
                            "include_all_devices": false,
                            "name": "devicegroup2"
                        },
                        {
                            "devices": [
                                {
                                    "include_all_ips": false,
                                    "ips": [
                                        "10.40.1.2"
                                    ],
                                    "name": "device1"
                                },
```

(continues on next page)

(continued from previous page)

```
                                {
                                    "name": "logsource",
                                    "include_all_ips": false,
                                    "ips": [
                                        "10.40.1.3"
                                    ]
                                }
                            ],
                            "include_all_devices": false,
                            "name": "devicegroup1"
                        }
                    ],
                    "logpoint_ip": "127.0.0.1",
                    "repos": [
                        "_logpoint"
                    ]
                }
            ]
        },
        "query": "col_type=syslog",
        "roles": "5bebd9fdd8aaa42840edc84e"
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

67.2 UserGroups - Edit

Edits a new user group in a Fabric-enabled LogPoint.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/UserGroups/{id}
```

Parameter

Field	Label in UI	Type	Description
description	Description	String	Description of usergroup. Optional Field
id	-	String	Existing Usergroup id . Obtain the value of the required Usergroup id using Usergroups - List API. Mandatory Field
name	Name	String	Name of usergroup. Mandatory Field

Continued on next page

Table 2 – continued from previous page

Field	Label in UI	Type	Description
object_permission	Object Permission	json	Mandatory Field. Specify permission for repos, usergroups, devices and ips. The following parameters should be provided to define object_permission. **include_all_permission**: Specifies full permission for repos and device_groups for all logpoints. If include_all_permission key is set as true, user should not give permission parameter in object_permission json. **permission**: List of jsons. To define permission, the following parameters should be provided. • *logpoint_ip*: Private IP of the logpoint. Use DistributedLogpoints - List API to obtain the private_ip of the required distributed logpoints. For localhost the logpoint_ip value is "127.0.0.1". Mandatory Field. • *include_all_repos*: Select/Unselect all repos for the given logpoint. If include_all_repos key is set as true, user should not give repos parameter. • *repos*: Name of the repos. Use Repos - FetchRemoteRepos API to obtain the names of the repos.

Table 2 – continued from previous page

Field	Label in UI	Type	Description
query	Universal Query	String	Universal Query for a user group. Optional Field
roles	Permission Group	String	Permission group. Mandatory Field

Request Example

```
{
    "data": {
        "description": "New usergroup",
        "name": "usergroup1",
        "object_permission": {
            "include_all_permission": false,
            "permission": [
                {
                    "include_all_device_groups": true,
                    "include_all_repos": true,
                    "logpoint_ip": "10.45.1.1"
                },
                {
                    "device_groups": [
                        {
                            "include_all_devices": true,
                            "name": "devicegroup3"
                        },
                        {
                            "devices": [
                                {
                                    "include_all_ips": true,
                                    "name": "device2"
                                }
                            ],
                            "include_all_devices": false,
                            "name": "devicegroup2"
                        },
                        {
                            "devices": [
                                {
                                    "include_all_ips": false,
                                    "ips": [
                                        "10.40.1.2"
                                    ],
                                    "name": "device1"
                                },
```

(continues on next page)

(continued from previous page)

```
                                {
                                    "name": "logsource",
                                    "include_all_ips": false,
                                    "ips": [
                                        "10.40.1.3"
                                    ]
                                }
                            ],
                            "include_all_devices": false,
                            "name": "devicegroup1"
                        }
                    ],
                    "logpoint_ip": "127.0.0.1",
                    "repos": [
                        "_logpoint"
                    ]
                }
            ]
        },
        "query": "col_type=syslog",
        "roles": "5bebd9fdd8aaa42840edc84e"
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

67.3 UserGroups - Get

Fetches a User Group with given ID.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/UserGroups/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	ID of the existing usergroup that you want to fetch.

Success Response

```
{
    "active": true,
    "description": "New usergroup",
    "id": "60e82304689d753ab310f1fe",
    "lpadmin": false,
    "name": "usergroup1",
    "object_permission": {
        "include_all_permission": false,
        "permitted": [
            {
                "device_groups": [
                    {
                        "devices": [
                            {
                                "ips": [
                                    "10.45.1.1"
                                ],
                                "name": "device1"
                            }
                        ],
                        "name": "devicegroup1"
                    }
                ],
                "logpoint_ip": "127.0.0.1",
                "logpoint_name": "LogPoint10",
                "repos": [
                    "_logpoint"
                ]
            },
            {
                "device_groups": [
                    {
                        "devices": [
                            {
                                "ips": [
                                    "10.3.4.5",
                                    "10.7.7.11"
                                ],
                                "name": "device2"
                            },
```

(continues on next page)

(continued from previous page)

```
                            {
                                "ips": [
                                    "10.7.8.1",
                                    "10.7.8.2"
                                ],
                                "name": "device3"
                            }
                        ],
                        "name": "devicegroup2"
                    }
                ],
                "logpoint_ip": "10.232.21.1",
                "logpoint_name": "LogPoint11",
                "repos": [
                    "_LogPointAlerts",
                    "_logpoint",
                    "default"
                ]
            }
        ]
    },
    "permission_group": "60dd435d3f7ba781e7035326",
    "query": "col_type=syslog",
    "tid": "",
    "useradmin": false,
    "users": []
}
```

67.4 UserGroups - List

Lists all existing User Groups.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/UserGroups
```

Success Response

```
[
    {
        "active": true,
        "description": "New usergroup",
        "id": "60e82304689d753ab310f1fe",
        "lpadmin": false,
```

(continues on next page)

(continued from previous page)

```
        "name": "usergroup1",
        "object_permission": {
            "include_all_permission": false,
            "permitted": [
                {
                    "device_groups": [
                        {
                            "devices": [
                                {
                                    "ips": [
                                        "10.45.1.1"
                                    ],
                                    "name": "device1"
                                }
                            ],
                            "name": "devicegroup1"
                        }
                    ],
                    "logpoint_ip": "127.0.0.1",
                    "logpoint_name": "LogPoint10",
                    "repos": [
                        "_logpoint"
                    ]
                },
                {
                    "device_groups": [
                        {
                            "devices": [
                                {
                                    "ips": [
                                        "10.3.4.5",
                                        "10.7.7.11"
                                    ],
                                    "name": "device2"
                                },
                                {
                                    "ips": [
                                        "10.7.8.1",
                                        "10.7.8.2"
                                    ],
                                    "name": "device3"
                                }
                            ],
                            "name": "devicegroup2"
                        }
```

(continues on next page)

(continued from previous page)

```
                    ],
                    "logpoint_ip": "10.232.21.1",
                    "logpoint_name": "LogPoint11",
                    "repos": [
                        "_LogPointAlerts",
                        "_logpoint",
                        "default"
                    ]
                }
            ]
        },
        "permission_group": "60dd435d3f7ba781e7035326",
        "query": "col_type=syslog",
        "tid": "",
        "useradmin": false,
        "users": []
    }
]
```

67.5 UserGroups - RefreshList

Syncs the current User Group List with LogPoint's User Group List.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/UserGroups/refreshlist
```

Request Example

```
{
    "data": {}
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

67.6 UserGroups - Trash

Removes the usergroup with given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/UserGroups/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	ID of the existing device that you want to delete. Mandatory Field

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

Note:

1. You can use the *Ungrouped* value in the *device_groups* parameter of the **UserGroups - Create** and **UserGroups - Edit** APIs to include the devices that do not belong to any device groups.
2. While configuring the user groups for remote LogPoint instances, if you are using the *Ungrouped* value then at least one of the given devices must not belong to any device group for the API to execute successfully.
3. You must execute the **UserGroups - RefreshList** API until the data in the API Server is synced with the Fabric-enabled LogPoint data in the following cases:

- After adding or deleting distributed LogPoints.
- After creating, editing, or deleting repos, device groups, and devices.
- After creating or editing user groups.

CHAPTER

SIXTYEIGHT

USERS

68.1 Users - Activate

Activates the user with given id .

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Users/{id}/activate
```

Parameter

Field	Label in UI	Type	Description
id	-	String	User id . Mandatory Field

Request Example

```
{
   "data": {}
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

68.2 Users - ChangePassword

Changes the password of user with given id.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Users/{id}/
↪changePassword
```

Parameter

Field	Label in UI	Type	Description
id	-	String	ID of the user whose password you want to change. Mandatory Field
new_password	New Password	String	New password. Mandatory Field

Request Example

```
{
   "data": {
      "new_password": "password1"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

68.3 Users - Create

Creates a new user in a Fabric-enabled LogPoint.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Users
```

Parameter

Field	Label in UI	Type	Description
email	Email	String	Valid email address of the user. Mandatory Field
firstname	Firstname	String	First name of the user. Mandatory Field

Continued on next page

Table 3 – continued from previous page

Field	Label in UI	Type	Description
lastname	Lastname	String	Last name of the user. Mandatory Field
password	Password	String	Username password . The password value should be at least 5 characters in length. Mandatory Field
timezone	Time Zone	String	An optional string value that specifies the given timezones by logpoint. Obtain the value of the available timezones using Timezone - List API. If no timezone is given, default timezone is set to "UTC". Optional Field
usergroup	Usergroup	[String]	List of usergroup ids. Mandatory Field
username	Username	String	Name of the user. Username should be unique and length value can be from 2 to 50 characters. Mandatory Field

Request Example

```
{
   "data": {
      "email": "william@lp.com",
      "firstname": "William",
      "lastname": "Smith",
      "password": "password",
      "timezone": "Asia/Kathmandu",
      "usergroup": [
         "5bebd9fdd8aaa42840edc850"
      ],
      "username": "UserA"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

68.4 Users - Deactivate

Deactivates the user with given id .

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Users/{id}/deactivate
```

Parameter

Field	Label in UI	Type	Description
id	-	String	User id . Mandatory Field

Request Example

```
{
   "data": {}
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

68.5 Users - Edit

Edits the user settings with given ID.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Users/{id}
```

Parameter

Field	Label in UI	Type	Description
email	Email	String	Valid email address of the user. Mandatory Field
firstname	Firstname	String	First name of the user. Mandatory Field

Continued on next page

Table 5 – continued from previous page

Field	Label in UI	Type	Description
id	-	String	Existing Device id . Obtain the value of the required Device id using Devices - List API. Mandatory Field
lastname	Lastname	String	Last name of the user. Mandatory Field
timezone	Time Zone	String	An optional string value that specifies the given timezones by logpoint. Obtain the value of the available timezones using Timezone - List API. If no timezone is given, default timezone is set to "UTC". Optional Field
usergroup	Usergroup	[String]	List of usergroup ids. Mandatory Field

Request Example

```
{
  "data": {
    "email": "william@lp.com",
    "firstname": "William",
    "lastname": "Smith",
    "timezone": "Asia/Kathmandu",
    "usergroup": [
      "5bebd9fdd8aaa42840edc850"
    ]
  }
}
```

Success Response

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

68.6 Users - FetchUsers

Lists all existing users.

DEPRECATED ! *Will be removed in future version. Use <b>Users - List</b> API instead.*

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Users/fetch
```

Request Example

```
{
   "data": {}
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}/{data_node}"
}
```

68.7 Users - Get

Fetches a User with given ID.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Users/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	ID of the existing user that you want to fetch.

Success Response

```
{
   "active": true,
   "dashboard": "4bebd9fdd8aaa42840ebc852",
   "email": "admin@logpoint.local",
   "failed_login_count": 0,
   "fields": {
      "automate_query_bar": [],
      "hidden_fields": [],
      "interesting_hidden_fields": [],
      "show_all": true
   },
   "firstname": "Admin",
   "fullname": "Admin Admin",
   "id": "4bebd9fdd8aaa42840edc553",
```

(continues on next page)

(continued from previous page)

```
    "last_login": {
        "login_date": "2020-11-30 04:36:41.983000"
    },
    "lastname": "Admin",
    "ldap_strategy": "",
    "locked": false,
    "locked_time": "2020-07-06 12:47:39.789000",
    "password_change_date": "2018-11-14 08:17:01.251000",
    "plugin_settings": {},
    "preferences": "5cebd9fdd8cac42840ddc82c",
    "query": "",
    "tid": "",
    "timezone": "UTC",
    "usergroup": [
        "4bebd8edd8aba42840edc85f",
        "4fb782bd40a18e4eb9e33a87"
    ],
    "username": "admin"
}
```

68.8 Users - List

Lists all existing Users.

GET

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Users
```

Success Response

```
[
    {
        "active": true,
        "dashboard": "4cebd9fcd8aaa42840e2c852",
        "email": "admin@logpoint.local",
        "failed_login_count": 0,
        "fields": {
            "automate_query_bar": [],
            "hidden_fields": [],
            "interesting_hidden_fields": [],
            "show_all": true
        },
        "firstname": "Admin",
        "fullname": "Admin Admin",
```

(continues on next page)

(continued from previous page)

```
            "id": "4cdcc8fdd8aaa42840edc851",
            "last_login": {
                "login_date": "2020-11-30 04:36:41.983000"
            },
            "lastname": "Admin",
            "ldap_strategy": "",
            "locked": false,
            "locked_time": "2020-07-06 12:47:39.789000",
            "password_change_date": "2018-11-14 08:17:01.251000",
            "plugin_settings": {},
            "preferences": "5bebd9faa8acc42840ede74a",
            "query": "",
            "tid": "",
            "timezone": "UTC",
            "usergroup": [
                "4cebd9fdd8aee42840edc83f",
                "4eb781cd40a19e5eb9e33a21"
            ],
            "username": "admin"
        }
]
```

68.9 Users - RefreshList

Syncs the current Users List with LogPoint's Users List.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Users/refreshlist
```

Request Example

```
{
    "data": {}
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

68.10 Users - Trash

Removes the user with given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Users/{id}
```

Parameter

Field	Label in UI	Type	Description
assigned_to_user	ASSIGN TO USER	String	ID of the user to whom the ownership of RBAC resources shall be transferred. Optional Field
force_delete	Delete	boolean	Value must be "true" to delete the users and their shared resources. Either force_delete or assigned_to_user must be present in the request while deleting the users who own any shared resources. Optional Field
id	-	String	ID of the existing user that you want to delete. You need to deactivate the user before deleting it. Mandatory Field

Request Example

```
{
   "data": {
      "force_delete": "false",
      "assigned_to_user": "5bfbd9faa8acc42840ede74b"
   }
}
```

Success Response

```
{
   "status": "Success",
   "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

68.11 Users - Unlock

Unlock the user with given id .

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/Users/{id}/unlock
```

Parameter

Field	Label in UI	Type	Description
id	-	String	User id . Mandatory Field

Request Example

```
{
    "data": {}
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

Note:

1. The **Users** API does not allow you to create and manage the plugin users for the authentication plugins. Currently, LogPoint supports the following authentication plugins:

   - LDAP Authentication
   - Radius Authentication
   - ADFS Authentication
   - SAML Authentication
   - OAuth Authentication

2. If a Fabric-enabled user is locked due to failed login attempts, you must execute the *Users - RefreshList* API to sync data with the Fabric-enabled LogPoint data.

CHAPTER

SIXTYNINE

WMIFETCHERPLUGIN

69.1 WMIFetcherPlugin - Create

Creates a WMI Fetcher using Device ID or Policy ID.

POST

https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/WMIFetcherPlugin

Parameter

Field	Label in UI	Type	Description
charset	Charset	String	Existing LogPoint charset. Obtain the value of the required charset using Charsets - List API. Mandatory Field
device_id	-	String	Device id . Obtain the value of the required Device id using Devices - List API. Optional Field
facility	Facility	String	One of the available facilities. Mandatory Field
interval	Fetch Interval (minutes)	int	Fetch interval in minutes. Mandatory Field
parser	Parser	String	Value must be "WmiParser"(exact). Mandatory Field
password	Password	String	WMI Fetcher password . Mandatory Field
policy_id	-	String	Respective LCP policy ID. Obtain the value of the required policy_id using LogCollectionPolicies - List API. Optional Field

Continued on next page

Table 1 – continued from previous page

Field	Label in UI	Type	Description
processpolicy	Processing Policy	String	Existing Processing Policy id or “None”. Obtain the value of the required Processing Policy id using ProcessingPolicy - List API. Mandatory Field
severity	Severity	String	One of the available severities. Mandatory Field
username	Username	String	WMI Fetcher username . Mandatory Field

Request Example

```
{
  "data": {
    "charset": "utf_8",
    "device_id": "57724aacd8aaa40b569bcb1f",
    "facility": "Kernel",
    "interval": 33,
    "parser": "WmiParser",
    "password": "hercules",
    "processpolicy": "57724aacd8aaa40b569bcb1fasd",
    "severity": "Emergency",
    "username": "TestWMIFetcher"
  }
}
```

Success Response

```
{
  "status": "Success",
  "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

69.2 WMIFetcherPlugin - Edit

Edits a WMI fetcher with given ID.

PUT

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/WMIFetcherPlugin/{id}
```

Parameter

Field	Label in UI	Type	Description
charset	Charset	String	Existing LogPoint charset. Obtain the value of the required charset using Charsets - List API. Mandatory Field
facility	Facility	String	One facility from the available facilities. Mandatory Field
id	-	String	WMI Fetcher Plugin uuid . To obtain the WMI fetcher uuid , execute Devices - List API if the collector was configured using device id or execute LogCollectionPolicies - List API if the collector was configured using log collection policy id . Mandatory Field
interval	Fetch Interval (minutes)	int	Fetch interval in minutes. Mandatory Field
parser	Parser	String	Value must be "WmiParser". Mandatory Field
password	Password	String	WMI Fetcher password . Mandatory Field
processpolicy	Processing Policy	String	Existing Processing Policy id or "None". Obtain the value of the required Processing Policy id using ProcessingPolicy - List API. . Mandatory Field
severity	Severity	String	One severity from the available severities. Mandatory Field
username	Username	String	WMI Fetcher username . Mandatory Field

Request Example

```
{
    "data": {
        "charset": "utf_8",
        "facility": "Kernel",
        "interval": 33,
        "parser": "WmiParser",
        "password": "hercules",
        "processpolicy": "57724aacd8aaa40b569bcb1fasd",
        "severity": "Emergency",
```

(continues on next page)

(continued from previous page)

```
        "username": "TestWMIFetcher"
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

69.3 WMIFetcherPlugin - TestExisting

Tests the existing WMI Fetcher connection.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/WMIFetcherPlugin/{id}
↪/testexistingwmi
```

Parameter

Field	Label in UI	Type	Description
id	-	String	WMI Fetcher Plugin uuid . Execute the Devices - List API to obtain the uuid of the required WMI Fetcher Plugin. Mandatory Field

Request Example

```
{
    "data": {}
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

69.4 WMIFetcherPlugin - TestNew

Tests newly created WMI fetcher connection.

POST

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/WMIFetcherPlugin/
↪testnewwmi
```

Parameter

Field	Label in UI	Type	Description
charset	Charset	String	Existing LogPoint charset. Obtain the value of the required charset using Charsets - List API. Mandatory Field
device_id	-	String	Device id . Obtain the value of the required Device id using Devices - List API. Mandatory Field
facility	Facility	String	One facility from the available facilities. Mandatory Field
interval	Fetch Interval (minutes)	int	Fetch interval in minutes. Mandatory Field
parser	Parser	String	Accepts only WmiParser (exact). Mandatory Field
password	Password	String	WMI Fetcher password . Mandatory Field
processpolicy	Processing Policy	String	Existing Processing Policy id . Obtain the value of the required Processing Policy id using ProcessingPolicy - List API. Mandatory Field
severity	Severity	String	One severity from the available severities. Mandatory Field
username	Username	String	WMI Fetcher username . Mandatory Field

Request Example

```
{
  "data": {
    "charset": "utf_8",
    "device_id": "57724aacd8aaa40b569bcb1f",
```

(continues on next page)

(continued from previous page)

```
        "facility": "Kernel",
        "interval": 33,
        "parser": "WmiParser",
        "password": "hercules",
        "processpolicy": "57724aacd8aaa40b569bcb1fasd",
        "severity": "Emergency",
        "username": "TestWMIFetcher"
    }
}
```

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```

69.5 WMIFetcherPlugin - Trash

Deletes the WMI fetcher with given ID.

DELETE

```
https://api-server-host-name/configapi/{pool_UUID}/{logpoint_identifier}/WMIFetcherPlugin/{id}
```

Parameter

Field	Label in UI	Type	Description
id	-	String	WMI Fetcher Plugin uuid . To obtain the WMI fetcher uuid , execute Devices - List API if the collector was configured using device id or execute LogCollectionPolicies - List API if the collector was configured using log collection policy id . Mandatory Field

Success Response

```
{
    "status": "Success",
    "message": "/monitorapi/{pool_UUID}/{logpoint_identifier}/orders/{request_id}"
}
```